Übersichtshandbuch

Identity Manager 4.0.2

Juni 2012

Novell

Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jede ausdrückliche oder implizite Garantie für Marktfähigkeit oder Eignung für einen bestimmten Zweck aus. Novell, Inc. behält sich das Recht vor, dieses Dokument jederzeit teilweise oder vollständig zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen davon in Kenntnis zu setzen.

Novell, Inc. gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jede ausdrückliche oder implizite Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software jederzeit ganz oder teilweise zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie stimmen zu, alle Gesetze zur Exportkontrolle einzuhalten und alle für den Export, Reexport oder Import von Lieferungen erforderlichen Lizenzen oder Klassifikationen zu erwerben. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Website Novell International Trade Services (http://www.novell.com/company/policies/trade_services). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Copyright © 2008–2012 Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch 5

1 Automatisierung von Geschäftsprozessen mit Identity Manager 7

1.1 Datensynchronisierung . . . 8
1.2 Workflow . . . 11
1.3 Rollen und Beglaubigung . . . 12
1.4 Selbstbedienung . . . 14
1.5 Revision, Berichterstellung und Konformität . . . 15

2 Funktionen von Identity Manager 4.0.2 17

2.1 Neue Funktionen von Identity Manager 4.0.2 . . . 17
2.2 Funktionen von Identity Manager 4.0.1 . . . 20
2.3 Funktionen von Identity Manager 4.0 . . . 21

3 Identity Manager-Familie 23

3.1 Identity Manager Advanced Edition . . . 24
3.2 Identity Manager Standard Edition . . . 24
3.3 Compliance Management-Plattform . . . 26
3.4 Aktivieren der Standard und Advanced Edition von Identity Manager . . . 27

4 Identity Manager-Architektur 29

4.1 Datensynchronisierung . . . 30
4.1.1 Komponenten . . . 31
4.1.2 Wichtige Konzepte . . . 32
4.2 Workflow, Rollen, Beglaubigung und Selbstbedienung . . . 35
4.2.1 Komponenten . . . 36
4.2.2 Wichtige Konzepte . . . 37
4.3 Revision und Berichterstellung . . . 38

5 Identity Manager-Werkzeuge 41

5.1 Analyzer . . . 42
5.2 Designer . . . 43
5.3 iManager . . . 45
5.4 Rollenzuordnungsadministrator . . . 45
5.5 Identitätsberichterstellung . . . 46

6 Aktionen in Identity Manager 49

6.1 Identitätsdepot . . . 50
6.2 Schnittstellenmodul . . . 52
6.3 Kanäle . . . 53
6.4 Ereignisse und Befehle . . . 53
6.5 Schemazuordnungsrichtlinie . . . 54
6.6 Ereignistransformationsregel . . . 54

6.6.1 Herausgeber . . . 55
6.6.2 Abonnent . . . 55
6.7 Filter . . . 55
6.7.1 Synchronisierungsattribut . . . 56
6.7.2 Benachrichtigungsattribut . . . 56
6.8 Hinzufügeprozessor . . . 57
6.8.1 Herausgeber . . . 57
6.8.2 Abonnent . . . 57
6.9 Übereinstimmungsregel . . . 58
6.9.1 Herausgeber . . . 58
6.9.2 Abonnent . . . 58
6.10 Erstellungsregel . . . 59
6.10.1 Herausgeber . . . 59
6.10.2 Abonnent . . . 59
6.11 Platzierungsregel . . . 59
6.11.1 Herausgeber . . . 60
6.11.2 Abonnent . . . 60
6.12 Befehlstransformationsregel . . . 60
6.12.1 Herausgeber . . . 60
6.12.2 Abonnent . . . 61
6.13 Regeln, Richtlinien und Formatvorlagen . . . 61
6.13.1 Eingabetransformationsregel . . . 63
6.13.2 Ausgabetransformationsregel . . . 63
6.13.3 Verknüpfungen . . . 64
6.13.4 Künstliches Hinzufügen . . . 64
6.13.5 Verarbeitung der Zusammenführung . . . 66

7 Weitere Schritte 71

7.1 Planen einer Identity Manager-Lösung . . . 71
7.2 Vorbereiten der Daten für die Synchronisierung . . . 71
7.3 Installation oder Aufrüstung von Identity Manager . . . 71
7.4 Konfigurieren von Identity Manager . . . 72
7.4.1 Datensynchronisierung . . . 72
7.4.2 Zuordnen von Rollen . . . 73
7.4.3 Konfiguration der Benutzeranwendung . . . 73
7.4.4 Konfigurieren von Revision, Berichterstellung und Konformität . . . 73
7.5 Identity Manager verwalten . . . 74

Informationen zu diesem Handbuch

Dieses Handbuch bietet eine Einführung in Novell Identity Manager, ein WorkloadIQ-Produkt, das die Verwaltung von Identitäten und Zugriffen in physischen, virtuellen sowie Cloud-Umgebungen ermöglicht. Es wird erläutert, wie Sie Geschäftsprobleme mithilfe von Identity Manager lösen und gleichzeitig Kosten einsparen sowie die Konformität sicherstellen können. Das Handbuch enthält außerdem einen technischen Überblick über die Komponenten und Werkzeuge von Identity Manager, die zum Erstellen Ihrer Identity Manager-Lösung zur Verfügung stehen. Dieses Handbuch gliedert sich wie folgt:

- Kapitel 1, „Automatisierung von Geschäftsprozessen mit Identity Manager“, auf Seite 7
- Kapitel 2, „Funktionen von Identity Manager 4.0.2“, auf Seite 17
- Kapitel 3, „Identity Manager-Familie“, auf Seite 23
- Kapitel 4, „Identity Manager-Architektur“, auf Seite 29
- Kapitel 5, „Identity Manager-Werkzeuge“, auf Seite 41
- Kapitel 6, „Aktionen in Identity Manager“, auf Seite 49
- Kapitel 7, „Weitere Schritte“, auf Seite 71

Zielgruppe

Dieses Handbuch ist für Administratoren, Berater und Netzwerktechniker gedacht, die eine detaillierte Einführung in die Geschäftslösungen, Technologien und Werkzeuge von Identity Manager benötigen.

Aktualisierungen der Dokumentation

Die neueste Version dieses Dokuments finden Sie auf der Website zur Identity Manager-Dokumentation (http://www.netiq.com/documentation/idm402/index.html).

Zusätzliche Dokumentation

Die Dokumentation für Identity Manager-Treiber finden Sie auf der Website für Identity Manager-Treiber (http://www.netiq.com/documentation/idm402drivers/index.html).

1 Automatisierung von Geschäftsprozessen mit Identity Manager

Nachfolgend werden einige der Geschäftsprozesse beschrieben, die Sie durch die Implementierung eines Novell Identity Manager-Systems automatisieren können. Wenn Sie die Identity Manager-Lösungen zur Automatisierung von Geschäftsprozessen bereits kennen, können Sie direkt mit der technischen Einführung unter Kapitel 4, „Identity Manager-Architektur“, auf Seite 29 fortfahren.

Das Verwalten von Identitätsanforderungen stellt in den meisten Unternehmen eine Kernfunktion dar. Stellen Sie sich beispielsweise einmal vor, es ist früh an einem Montagmorgen. Sie gehen die Liste der Anforderungen in Ihrer Warteschlange durch:

- Die Handynummer von Joachim Schmidt hat sich geändert. Sie müssen sie in der Personaldatenbank und in vier weiteren unabhängigen Systemen aktualisieren.
- Karen Hansen, die gerade aus einem längeren Urlaub zurückgekehrt ist, hat ihr Email-Passwort vergessen. Sie müssen ihr helfen, es wiederzuerlangen oder zurückzusetzen.
- Hans Müller hat gerade einen neuen Mitarbeiter eingestellt. Sie müssen für den neuen Mitarbeiter den Netzwerkzugriff und ein Email-Konto einrichten.
- Ida Moser benötigt Zugriff auf die Oracle-Finanzdatenbank, wofür Sie die Genehmigung von drei verschiedenen Vorgesetzten einholen müssen.
- Robert Meyer hat von der Buchhaltung in die Rechtsabteilung gewechselt. Sie müssen dafür sorgen, dass er Zugriff auf dieselben Ressourcen erhält wie die übrigen Mitarbeiter der Rechtsabteilung und dass sein Zugriff auf die Buchhaltungsressourcen gesperrt wird.
- Karl Jonas, Ihr eigener Chef, hat eine Kopie von Ida Mosers Bitte um Zugriff auf die Oracle-Finanzdatenbank erhalten und überlegt, ob nicht zu viele Mitarbeiter Zugriff darauf besitzen. Sie müssen für ihn einen Bericht erstellen, in dem alle Mitarbeiter mit Zugriff auf die Datenbank aufgeführt sind.

Sie atmen tief durch und beginnen mit der ersten Anforderung, wobei Ihnen bewusst ist, dass es schwierig wird, allen Anforderungen rechtzeitig nachzukommen, und dass Sie daneben kaum Zeit finden werden, Ihre anderen Projekte fertigzustellen.

Wenn dies für Sie oder Kollegen in Ihrem Unternehmen nach einem ganz normalen Arbeitstag klingt, ist Identity Manager die richtige Lösung für Sie. Die Kernfunktionen von Identity Manager, die auf der folgenden Abbildung vorgestellt werden, können Ihnen helfen, all diese Aufgaben und noch weitere zu automatisieren. Die Komponenten „Workflows“, „Rollen“, „Beglaubigung“, „Selbstbedienung“, „Revision“ und „Berichterstellung“ verwenden die durch Ihre Geschäftsrichtlinien gesteuerte Datensynchronisierung zwischen mehreren Systemen, um die Prozesse zu automatisieren, die für die Bereitstellung für Benutzer und die Passwortverwaltung erforderlich sind – zwei der schwierigsten und zeitintensivsten Aufgaben einer IT-Organisation.

Abbildung 1-1 *Kernfunktionen von Identity Manager*

In den folgenden Abschnitten werden diese Funktionen von Identity Manager vorgestellt und es wird erläutert, wie sie Ihnen dabei helfen können, den Identitätsanforderungen Ihrer Organisation gerecht zu werden:

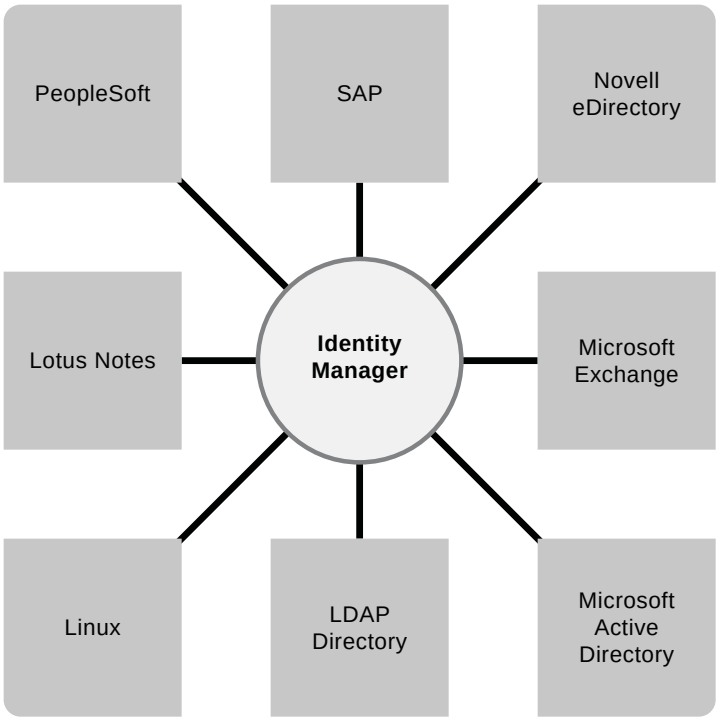
- Abschnitt 1.1, „Datensynchronisierung“, auf Seite 8
- Abschnitt 1.2, „Workflow“, auf Seite 11
- Abschnitt 1.3, „Rollen und Beglaubigung“, auf Seite 12
- Abschnitt 1.4, „Selbstbedienung“, auf Seite 14
- Abschnitt 1.5, „Revision, Berichterstellung und Konformität“, auf Seite 15

1.1 Datensynchronisierung

In den meisten Organisationen sind Identitätsdaten in verschiedenen Systemen gespeichert. Möglicherweise sind bei Ihnen Identitätsdaten aber nur in einem System gespeichert, und Sie benötigen sie auch in einem anderen System. In beiden Fällen ist es erforderlich, dass Sie Daten schnell zwischen verschiedenen Systemen übertragen und synchronisieren können.

Mit Identity Manager können Sie Informationen über eine Vielzahl an Anwendungen, Datenbanken, Betriebssystemen und Verzeichnissen hinweg synchronisieren, transformieren und verteilen, z. B. Daten aus SAP, PeopleSoft, Salesforce, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, Novell eDirectory, Linux und UNIX sowie LDAP-Verzeichnissen.

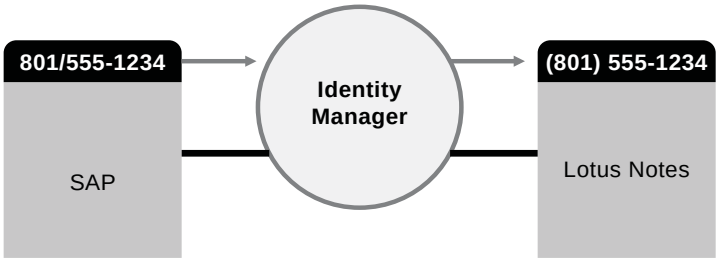
Abbildung 1-2 *Verbinden mehrerer Systeme mit Identity Manager*



Sie steuern den Datenfluss zwischen den verbundenen Systemen. Unter anderem bestimmen Sie, welche Daten gemeinsam genutzt werden, welches System die autorisierte Quelle für bestimmte Daten ist und wie die Daten interpretiert und transformiert werden, um den Anforderungen anderer Systeme gerecht zu werden.

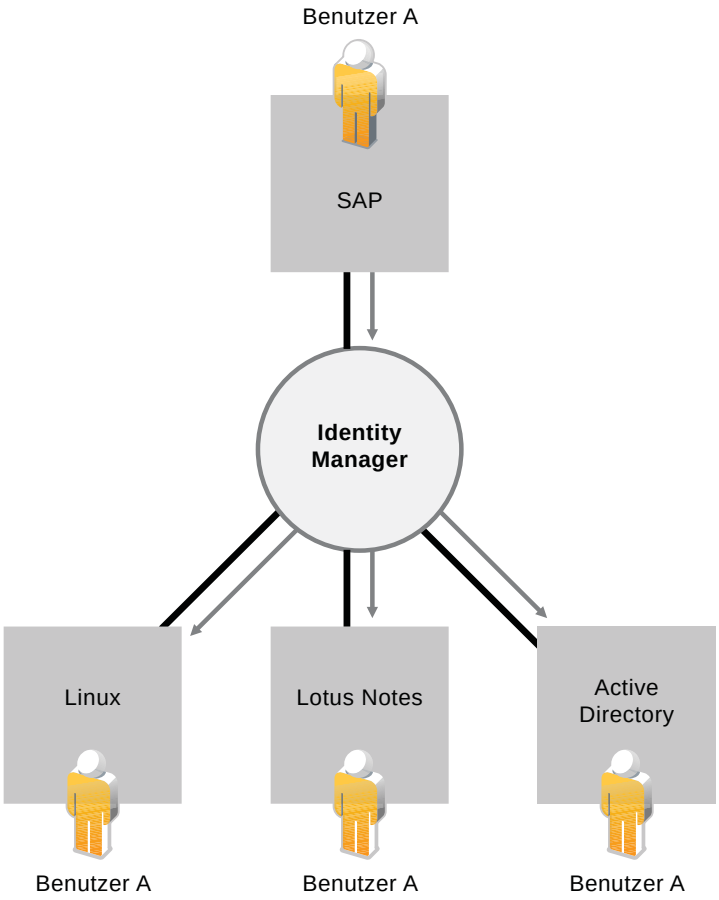
Im nachfolgenden Diagramm ist die SAP-Personaldatenbank die autorisierte Quelle für die Telefonnummer eines Benutzers. Das Lotus Notes-System verwendet ebenfalls Telefonnummern, daher wandelt Identity Manager die Nummer in das erforderliche Format um und überträgt sie an das Lotus Notes-System. Jedes Mal, wenn die Telefonnummer im SAP-Personalsystem geändert wird, werden die Daten im Lotus Notes-System synchronisiert.

Abbildung 1-3 *Datensynchronisierung verbundener Systeme*



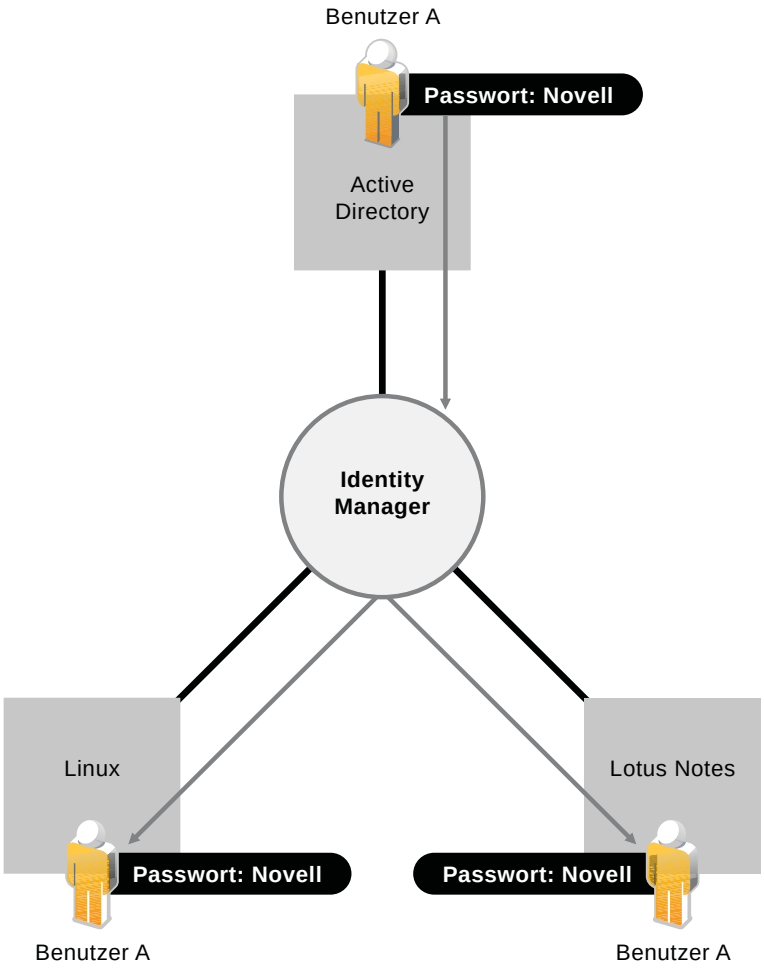
Das Verwalten der Daten vorhandener Benutzer stellt nur die erste Ebene der Datensynchronisierungsfunktionen von Identity Manager dar. Zusätzlich können mit Identity Manager in Verzeichnissen wie Active Directory, auf Systemen wie PeopleSoft und Lotus Notes und unter Betriebssystemen wie UNIX und Linux neue Benutzerkonten erstellt und vorhandene Konten entfernt werden. Wenn Sie beispielsweise einen neuen Mitarbeiter zu Ihrem SAP-Personalsystem hinzufügen, kann Identity Manager automatisch ein neues Benutzerkonto in Active Directory, ein neues Konto in Lotus Notes und ein neues Konto in einem Linux NIS-Kontenverwaltungssystem erstellen.

Abbildung 1-4 *Erstellung von Benutzerkonten in verbundenen Systemen*



Im Rahmen der Datensynchronisierungsfunktion kann Identity Manager Sie auch bei der Synchronisierung von Passwörtern zwischen verschiedenen Systemen unterstützen. Wenn ein Benutzer beispielsweise sein Passwort in Active Directory ändert, kann Identity Manager diese Änderung an Lotus Notes und Linux weitergeben.

Abbildung 1-5 *Passwortsynchronisierung verbundener Systeme*

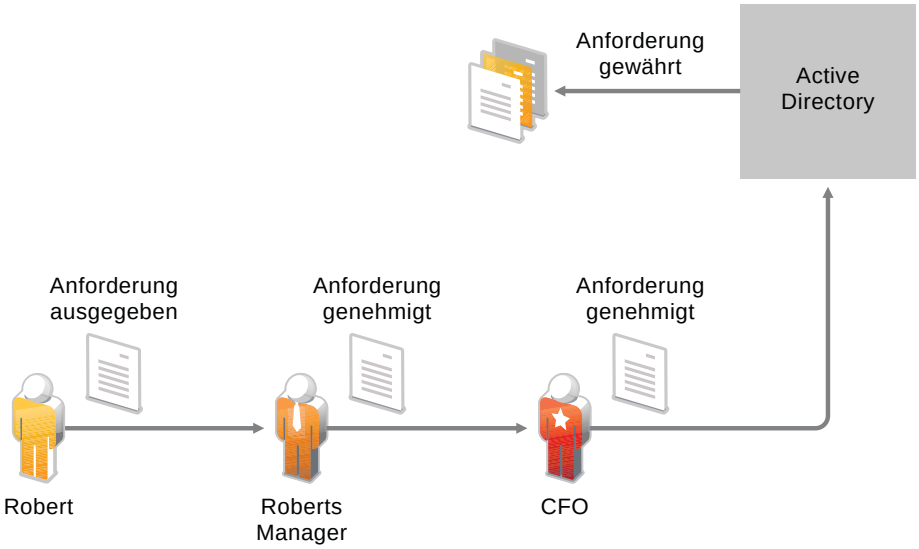


1.2 Workflow

Wahrscheinlich ist für den Zugriff auf viele Ressourcen in Ihrer Organisation keine Genehmigung erforderlich. Möglicherweise ist der Zugriff auf einige Ressourcen jedoch beschränkt und muss von einer oder mehreren Personen genehmigt werden.

Identity Manager bietet Workflow-Funktionen, die sicherstellen, dass bei Ihren Bereitstellungsprozessen die richtigen Ressourcen-Genehmiger einbezogen werden. Nehmen Sie beispielsweise an, dass Robert, für den bereits ein Active Directory-Konto eingerichtet wurde, über Active Directory auf Finanzberichte zugreifen muss. Dies muss von Roberts unmittelbarem Vorgesetzten sowie vom Leiter der Finanzabteilung genehmigt werden. Hierzu können Sie einen Genehmigungsworkflow einrichten, der Roberts Anforderung zunächst an seinen Vorgesetzten und sobald dieser die Genehmigung erteilt hat an den Leiter der Finanzabteilung weiterleitet. Wenn der Leiter der Finanzabteilung seine Genehmigung erteilt hat, wird die automatische Bereitstellung der von Robert zum Zugriff und zur Ansicht der Finanzdokumente benötigten Active Directory-Rechte veranlasst.

Abbildung 1-6 *Genehmigungsworkflow für die Bereitstellung für Benutzer*



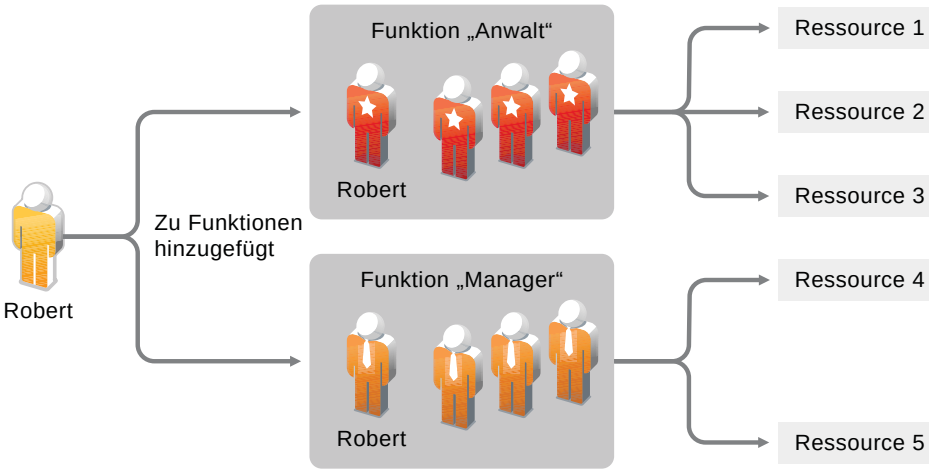
Workflows können automatisch initiiert werden, sobald ein bestimmtes Ereignis eintritt (z. B. wenn ein neuer Benutzer zu Ihrem Personalsystem hinzugefügt wird), oder sie können manuell durch eine Benutzeranforderung initiiert werden. Sie können sicherstellen, dass Genehmigungen rechtzeitig erteilt werden, indem Sie Vertretungsgenehmiger und Genehmigungsteams einrichten.

1.3 Rollen und Beglaubigung

Oft hängt es von der Funktion eines Mitarbeiters in einer Organisation ab, auf welche Ressourcen er Zugriff benötigt. Zum Beispiel benötigen die Anwälte einer Kanzlei vermutlich auf andere Ressourcen Zugriff als die Anwaltsgehilfen.

Mit Identity Manager können Sie die Bereitstellung für Benutzer abhängig von deren Rolle innerhalb der Organisation durchführen. Definieren Sie Rollen und nehmen Sie Zuweisungen entsprechend den Anforderungen Ihrer Organisation vor. Wenn einem Benutzer eine Rolle zugewiesen wird, stellt Identity Manager für den Benutzer den Zugriff auf die Ressourcen bereit, die der Rolle zugeordnet sind. Wenn einem Benutzer mehrere Rollen zugewiesen werden, erhält er Zugriff auf alle Ressourcen, die diesen Rollen zugewiesen sind, wie in der folgenden Abbildung dargestellt ist:

Abbildung 1-7 *Rollenbasierte Bereitstellung von Ressourcen*



Sie können festlegen, dass Benutzer automatisch Rollen hinzugefügt werden, wenn in Ihrer Organisation ein bestimmtes Ereignis eintritt (z. B. wenn ein neuer Benutzer mit der Stellenbezeichnung „Anwalt“ zu Ihrer SAP-Personaldatenbank hinzugefügt wird). Wenn für das Hinzufügen eines Benutzers zu einer Rolle eine Genehmigung erforderlich ist, können Sie Workflows einrichten, mit deren Hilfe Rollenanforderungen an die entsprechenden Genehmiger weitergeleitet werden. Sie können Benutzer auch manuell zu Rollen hinzufügen.

Es kann vorkommen, dass bestimmte Rollen nicht derselben Person zugewiesen werden dürfen, da die Rollen im Widerspruch zueinander stehen. Identity Manager bietet die Möglichkeit zur Funktionstrennung, mit deren Hilfe Sie verhindern können, dass Benutzern widersprüchliche Rollen zugewiesen werden, sofern nicht ein Mitarbeiter Ihrer Organisation eine Ausnahme für den Konflikt macht.

Da Rollenzuweisungen den Zugriff der Benutzer auf die Ressourcen Ihrer Organisation festlegen, ist es äußerst wichtig, die Korrektheit der Zuweisungen sicherzustellen. Falsche Zuweisungen können die Einhaltung von Unternehmens- und behördlichen Bestimmungen gefährden. Mit Identity Manager können Sie die Richtigkeit der Rollenzuweisungen durch einen Beglaubigungsprozess validieren. Mithilfe dieses Prozesses zertifizieren die verantwortlichen Mitarbeiter innerhalb Ihrer Organisation die den Rollen zugewiesenen Daten:

- **Benutzerprofilbeglaubigung:** Ausgewählte Benutzer bestätigen ihre eigenen Profilinformationen (Vorname, Nachname, Stellenbezeichnung, Abteilung, Email-Adresse usw.) und korrigieren falsche Angaben. Die Richtigkeit der Profilinformationen ist für korrekte Rollenzuweisungen ausschlaggebend.
- **Funktionstrennungsverletzungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Funktionstrennungsverletzungsbericht und bestätigen die Richtigkeit des Berichts. In dem Bericht sind alle Ausnahmen aufgeführt, die es erlauben, einem Benutzer widersprüchliche Rollen zuzuweisen.
- **Rollenzuweisungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Bericht, in dem ausgewählte Rollen zusammen mit den Benutzern, Gruppen und Rollen aufgeführt sind, die den einzelnen Rollen zugewiesen sind. Die verantwortlichen Mitarbeiter müssen dann die Korrektheit der Informationen bestätigen.
- **Benutzerzuweisungsbeglaubigung:** Verantwortliche Mitarbeiter prüfen einen Bericht, in dem ausgewählte Benutzer zusammen mit den Rollen aufgeführt sind, denen sie zugewiesen sind. Die verantwortlichen Mitarbeiter müssen dann die Korrektheit der Informationen bestätigen.

Diese Beglaubigungsberichte sollen Ihnen in erster Linie dabei helfen, sicherzustellen, dass die Rollenzuweisungen korrekt sind und dass es gültige Gründe für das Zulassen von Ausnahmen für widersprüchliche Rollen gibt.

1.4 Selbstbedienung

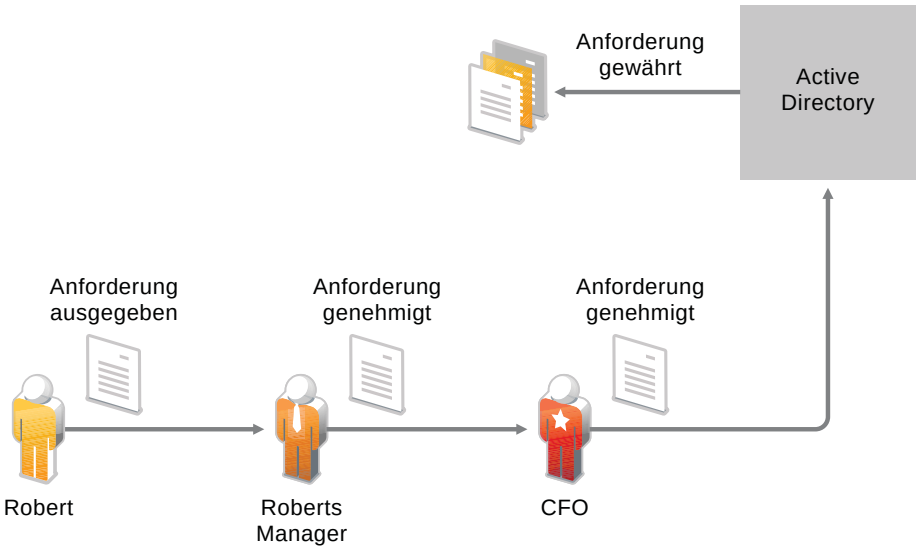
Vermutlich gibt es bei Ihnen Vorgesetzte und Abteilungen, die ihre Benutzerinformationen und Zugriffsanforderungen lieber selbst verwalten würden, als dies Ihnen oder Ihren Mitarbeitern zu überlassen. Wie oft haben Sie schon Sätze gehört wie, „Warum kann ich meine Handynummer in unserem Unternehmensverzeichnis nicht selbst ändern?“ Oder: „Ich arbeite in der Marketing-Abteilung. Warum muss ich den Helpdesk anrufen, um Zugriff auf die Marketing-Informationsdatenbank zu erhalten?“

Mit Identity Manager können Sie administrative Aufgaben an die Mitarbeiter delegieren, die dafür zuständig sein sollten. Zum Beispiel können Sie einzelnen Benutzern Folgendes ermöglichen:

- Das Verwalten ihrer persönlichen Daten im Unternehmensverzeichnis. Statt sich an Sie zu wenden, um eine Handynummer ändern zu lassen, können die Benutzer diese an einer Stelle ändern und die Änderung an alle Systeme weitergeben, die Sie über Identity Manager synchronisiert haben.
- Das Ändern ihrer Passwörter, das Einrichten eines Tipps für vergessene Passwörter sowie das Einrichten von Sicherheitsabfragen und -antworten für vergessene Passwörter. Statt Sie zu bitten, ein vergessenes Passwort zurückzusetzen, können die Benutzer dies selbst tun, nachdem sie einen Tipp erhalten oder eine Sicherheitsabfrage beantwortet haben.
- Das Anfordern von Zugriff auf Ressourcen wie Datenbanken, Systeme und Verzeichnisse. Die Benutzer müssen sich nicht mehr an Sie wenden, um den Zugriff auf eine Anwendung zu erhalten, sondern sie können die entsprechende Anwendung aus einer Liste von verfügbaren Ressourcen auswählen.

Zusätzlich zur Selbstbedienung für einzelne Benutzer bietet Identity Manager eine Selbstbedienungsverwaltung für Funktionen (Verwaltung, Helpdesk usw.) an, die für die Unterstützung, die Überwachung und die Genehmigung von Benutzeranforderungen verantwortlich sind. Betrachten Sie beispielsweise das unter Abschnitt 1.2, „Workflow“, auf Seite 11 verwendete und nachfolgend dargestellte Szenario.

Abbildung 1-8 *Bereitstellungs-Workflow mit Selbstbedienung*



Die Selbstbedienungsfunktion von Identity Manager wird nicht nur von Robert dazu verwendet, Zugriff auf die benötigten Dokumente anzufordern, sondern auch sein Vorgesetzter und der Leiter der Finanzabteilung verwenden sie für die Genehmigung der Anforderung. Der eingerichtete Genehmigungsworkflow ermöglicht Robert, seine Anforderung zu initiieren und ihren Fortschritt zu überwachen, und Roberts Vorgesetztem und dem Leiter der Finanzabteilung, auf seine Anforderung zu antworten. Wenn die Anforderung von Roberts Vorgesetztem und dem Leiter der Finanzabteilung genehmigt wird, veranlasst dies die Bereitstellung der von Robert zum Zugriff und zur Ansicht der Finanzdokumente benötigten Active Directory-Rechte.

1.5 Revision, Berichterstellung und Konformität

Ohne Identity Manager kann die Bereitstellung für Benutzer ein mühsamer, zeitaufwändiger und kostenintensiver Vorgang sein. Einen noch bedeutend größeren Aufwand bringt es allerdings mit sich, zu überprüfen, ob die Bereitstellungsaktivitäten gemäß den Richtlinien, Anforderungen und Bestimmungen Ihrer Organisation erfolgen. Haben die richtigen Mitarbeiter Zugriff auf die richtigen Ressourcen? Haben die falschen Mitarbeiter keinen Zugriff auf dieselben Ressourcen? Hat der neue Mitarbeiter Zugriff auf das Netzwerk, seine Emails und die sechs weiteren für seine Arbeit erforderlichen Systeme? Wurde der Zugriff für den Mitarbeiter, der die Firma letzte Woche verlassen hat, gesperrt?

Mit Identity Manager haben Sie die Gewissheit, dass alle Benutzerbereitstellungsaktivitäten - vorangegangene und aktuelle - verfolgt und zu Revisionszwecken protokolliert werden. Identity Manager verfügt über ein intelligentes Repository mit Informationen über den aktuellen und den gewünschten Status des Identitätsdepots sowie der verwalteten Systeme in Ihrer Organisation. Aus diesem Warehouse können Sie jederzeit alle Informationen abrufen, die für die Einhaltung der für Ihre Organisation geltenden geschäftlichen Regeln und Richtlinien erforderlich sind.

Das Warehouse gibt Ihnen einen Gesamtüberblick über alle Geschäftsberechtigungen und Aufschluss darüber, welche Autorisierungen und Berechtigungen den Identitäten in Ihrer Organisation in der Vergangenheit und gegenwärtig erteilt wurden. Somit haben Sie die Gewissheit, dass Sie für die Einhaltung selbst anspruchsvollster GRC-Richtlinien gerüstet sind.

Identity Manager enthält vordefinierte Berichte für Identitätsinformations-Warehouse-Abfragen zur Sicherstellung der Einhaltung von Geschäfts-, IT- und Firmenrichtlinien. Sie können auch benutzerdefinierte Berichte erstellen, falls die vordefinierten Berichte für Ihre Anforderungen nicht geeignet sind.

2 Funktionen von Identity Manager 4.0.2

Novell Identity Manager 4.0.2 bietet ein intelligentes Identity-Framework, das Ihre vorhandenen IT-Assets und neue Computing-Modelle, z. B. „Software As a Service (SaaS)“, nutzt und somit Kosteneinsparungen ermöglicht sowie die Konformität zwischen physischen, virtuellen und Cloud-Umgebungen sicherstellt. Mithilfe von Novell Identity Manager-Lösungen können Sie sicherstellen, dass Ihre Organisation über die aktuellsten Benutzeridentitätsinformationen verfügt. Sie behalten die Kontrolle auf Unternehmensebene, indem Sie Identitäten innerhalb der Firewall und cloud-übergreifend verwalten, bereitstellen bzw. die Bereitstellung aufheben. Identity Manager ermöglicht Ihnen, auch Clouds in die Konformitätsverwaltung mit einzubeziehen.

Identity Manager 4.0.2 ist mit umfassenden Funktionen zum Vorkonfigurieren und Anpassen der Identity Manager-Treiberrichtlinien ausgestattet. Hierzu gehören das Identitätsmanagement und die Rollenverwaltung sowie Berichterstellungs- und Paketverwaltungsfunktionen. Sie können darüber hinaus Sicherheitsrichtlinien auf mehrere Systemdomänen anwenden. Identity Manager ermöglicht Ihnen die Benutzerverwaltung bei einer wachsenden Zahl an behördlichen Regelungen und gesetzlichen Bestimmungen. Es bietet mehr Schutz durch strategische Benutzerbereitstellungen und erfüllt somit den wachsenden Sicherheitsbedarf innerhalb der Firewall und in der Cloud-Umgebung. Das intelligente Identity-Framework bietet die Möglichkeit, Ihre vorhandene Infrastruktur mit neuen Computing-Modellen wie SaaS zu kombinieren.

- Abschnitt 2.1, „Neue Funktionen von Identity Manager 4.0.2“, auf Seite 17
- Abschnitt 2.2, „Funktionen von Identity Manager 4.0.1“, auf Seite 20
- Abschnitt 2.3, „Funktionen von Identity Manager 4.0“, auf Seite 21

2.1 Neue Funktionen von Identity Manager 4.0.2

- **Neue Treiber:**
  - **Bidirektionaler eDirectory-Treiber:** Der bidirektionale eDirectory-Treiber von Identity Manager synchronisiert Daten zwischen dem Identitätsdepot und eDirectory. Weitere Informationen hierzu finden Sie im *Identity Manager 4.0.2 Driver for Bidirectional eDirectory Implementation Guide* (Implementierungshandbuch für den Identity Manager 4.0.2-Treiber für bidirektionales eDirectory).
  - **Sentinel Identity Tracking Driver Implementation Guide (Implementierungshandbuch für den Sentinel Identity Tracking-Treiber):** Der Sentinel Identity Tracking-Treiber (Treiber für Identitätsüberwachung) ermöglicht die Integration mit Identity Manager und Sentinel zum Nachverfolgen von Benutzerkontoinformationen. Jedes Benutzerkonto kann mehrere Kontokennungen für jedes System in der Identity Manager-Lösung besitzen. Der Treiber verfolgt jede Kontokennung und sendet diese Informationen an Sentinel. Sentinel kann Berichte ausführen, um einzelne Kontokennungen einem bestimmten Benutzer zuzuordnen. Weitere Informationen finden Sie im *Driver for Sentinel Implementation Guide* (Implementierungshandbuch für den Treiber für Sentinel).

- **Funktionen für die Passwortverwaltung:**
  - **Verbesserungen der Passwortrichtlinie:** Identity Manager unterstützt nun drei neue Syntaxoptionen für die Passwortrichtlinie:
    - Verwendung der Microsoft-Passwortkomplexitätsrichtlinie
    - Verwendung der Passwortrichtlinie von Microsoft Server 2008
    - Verwendung der Novell-Syntax

    Weitere Informationen finden Sie unter „Supported Password Policy Syntax“ (Unterstützte Syntax für die Passwortrichtlinie) im *Identity Manager 4.0.2 Password Management Guide* (Handbuch zur Identity Manager 4.0.2 Passwortverwaltung).
- **Funktionen für den Rollenzuordnungsadministrator:**
  - **Synchronisierung der Codezuordnung:** Identity Manager 4.0.2 bietet Funktionen zur Synchronisierung der Codezuordnungstabellen zwischen dem Rollenzuordnungsadministrator und dem rollenbasierten Bereitstellungsmodul. Bei der Erstellung von Zuordnungen im Rollenzuordnungsadministrator können Sie eine Aktualisierung der Codezuordnung entweder im Rollenzordnungsadministrator oder im rollenbasierten Bereitstellungsmodul auslösen, falls die Codezuordnungen nicht übereinstimmen. Eine Aktualisierung der Rollenzuordnungen kann sehr lange dauern, wenn sie für alle Treiber und Berechtigungen ausgeführt wird. Daher haben Sie mit dem Rollenzuordnungsadministrator die Möglichkeit, eine Aktualisierung nur für die Berechtigungen auszulösen, die nicht übereinstimmen. Das rollenbasierte Bereitstellungsmodul stellt auch neue SOAP-Endpunkte zum Auslösen von Aktualisierungen der Rollenzuordnungen zur Verfügung. Weitere Informationen über die Änderungen beim Rollenzuordnungsadministrator finden Sie unter „Creating Role Resource Mappings“ (Erstellen von Rollenressourcenzuordnungen) im *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* (Benutzerhandbuch für den Rollenzuordnungsadministrator in Novell Identity Manager 4.0.2). Weitere Informationen über die neuen SOAP-Endpunkte finden Sie unter „Resource Web Service (Ressourcenwebdienst) “ im *User Application: Administration Guide* (Benutzeranwendung: Administrationshandbuch).
  - **Einstellungen zur Ressourcenerstellung für den Rollenzuordnungsadministrator:** Der Rollenzuordnungsadministrator stellt nun verschiedene Einstellungen für die Ressourcenerstellung bereit, mit denen Sie dem Treibernamen und dem Namen des logischen Systems beim Erstellen von Ressourcen ein Präfix hinzufügen können. Die Einstellungen zur Ressourcenerstellung ermöglichen es Ihnen auch, eine Ressourcenkategorie für automatisch erstellte Ressourcen auszuwählen. Weitere Informationen finden Sie unter „Customizing the Resource Names“ (Anpassen der Ressourcennamen) im *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* (Benutzerhandbuch für den Rollenzuordnungsadministrator in Novell Identity Manager 4.0.2).
- **Funktionen des rollenbasierten Provisioning-Moduls:**
  - **Genehmigungsverfahren für den Rollenentzug:** Das rollenbasierte Bereitstellungsmodul unterstützt nun die Anwendung von Genehmigungsverfahren für den Rollenentzug. Das Genehmigungsverfahren für Rollenentzugsanforderungen sowie die Liste der Genehmiger entsprechen der Vorgehensweise bei der Rollenerteilung. Wenn Sie angegeben haben, dass das Genehmigungsverfahren entsprechend der Standarddefinition der Rollenzuweisungsgenehmigung ausgeführt werden soll, dann wird dieses Verfahren angewendet. Alternativ können Sie ein benutzerdefiniertes Genehmigungsverfahren sowohl für Rollenerteilungsanforderungen als auch für Rollenentzugsanforderungen

angeben. Weitere Informationen finden Sie unter „Defining the Approval Process for a Role“ (Definieren des Genehmigungsprozesses für eine Rolle) im *User Application: User Guide* (Benutzeranwendung: Benutzerhandbuch).

- **Optimierung der Rollenlöschvorgänge:** Das rollenbasierte Bereitstellungsmodul hat den Prozess der Löschung von Rollen optimiert. Wenn Sie der Benutzeranwendung die Anweisung geben, eine Rolle zu löschen, wird zunächst der Rollenstatus auf „Anstehende Löschung“ festgelegt. Der Rollen- und Ressourcenservice-Treiber bemerkt anschließend die Statusänderung und führt die folgenden Schritte aus:

  1. Entfernt die Ressourcenzuweisungen für die Rolle
  2. Löscht die Rolle selbst

  Weitere Informationen finden Sie unter „Deleting Roles (Löschen von Rollen) “ im *User Application: User Guide* (Benutzeranwendung: Benutzerhandbuch).

- **SAML-Unterstützung für 64-Bit-Plattformen** SAML-Unterstützung für Single Sign-On wurde für 64-Bit-Linux- und -Windows-Plattformen hinzugefügt Weitere Informationen finden Sie unter „Single Sign On (SSO) Configuration“ (SSO-Konfiguration) im *User Application: Administration Guide* (Benutzeranwendung: Benutzerhandbuch).

- **Funktionen für das Identitätsberichterstellungsmodul:**
  - **Unterstützung für EAS unter Red Hat Enterprise Linux:** Der Event Auditing Service (EAS) wird nun unter Red Hat Enterprise Linux 5.7 und 6.0 (32-Bit und 64-Bit) ausgeführt.
  - **Neuer Rollenhierarchiebericht:** Der Rollenhierarchiebericht wurde dem Identitätsberichterstellungsmodul hinzugefügt. In diesem Bericht werden die Inhalte der Rollenhierarchie angezeigt sowie die mit den einzelnen Rollen verknüpften Ressourcen. Weitere Informationen finden Sie im Abschnitt „Role Hierarchy“ (Rollenhierarchie) unter *Using Identity Manager 4.0.2 Reports* (Verwenden von Identity Manager 4.0.2-Berichten).
  - **Möglichkeit zum Entfernen historischer Daten aus der Berichterstellungsdatenbank:**

    Mit dem Identitätsberichterstellungsmodul können Sie nun historische Daten aus der Berichterstellungsdatenbank entfernen. Wenn das Berichterstellungsmodul einen Vorgang zum Entfernen von Daten durchführt, werden nur die Daten aus Verlaufstabellen entfernt, die älter sind als der angegebene Aufbewahrungswert. Alle Verlaufsdaten, die jünger sind als die erlaubten Aufbewahrungsintervalle, werden weiterhin aufbewahrt. Der Vorgang zum Entfernen der Daten entfernt keine aktuellen Daten. Weitere Informationen finden Sie unter „Configuring Settings and Data Collection“ (Konfigurieren von Einstellungen und Datensammlung) im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

- **Designer-Funktionen:**
  - **REST-Aktivitätsunterstützung für Workflows** Designer 4.0.2 verfügt jetzt über eine neue Aktivität im Provisioning Request Definition-Editor (Provisioning-Anforderungsdefinitions-Editor), die es Benutzern ermöglicht, beim Verarbeiten von Workflowdaten REST-Endpunkte oder -Ressourcen aufzurufen. Mithilfe der REST-Aktivität können Workflows Daten mit REST-Diensten in und außerhalb der Organisation austauschen, und Benutzer können von einem REST-Dienst empfangene Daten als Entscheidungshilfe in Genehmigungsformularen verwenden.

    Weitere Informationen finden Sie im Abschnitt „Rest Activity“ (REST-Aktivität) im *User Application: Design Guide* (Benutzeranwendung: Entwurfshandbuch).
  - **Verbesserungen bei der Integrations-Aktivität für Workflows** Designer 4.0.2 enthält verschiedene Verbesserungen an der Integrations-Aktivität im Provisioning Request Definition-Editor, wie das Auflösen von Animationsfehlern und das Reduzieren der Größe

bereitgestellter PRDs. Außerdem können Benutzer jetzt mithilfe der Integrations-Aktivität SOAP-Anforderungen für die Aktivität in der Designer-Benutzeroberfläche leichter generieren.

Weitere Informationen finden Sie im Abschnitt „Adding an Integration Activity“ (Hinzufügen einer Integrations-Aktivität) im *User Application: Design Guide* (Benutzeranwendung: Entwurfshandbuch).

- **Leistungsverbesserungen in Designer** Designer 4.0.2 verfügt über verschiedene Verbesserungen bei der Leistung. Dazu gehören eine bessere Leistung beim Verwenden der verschiedenen im Produkt enthaltenen Editoren, eine verbesserte Darstellung der Konfigurationsseiten in der Benutzeroberfläche, eine höhere Geschwindigkeit von Project Checker sowie gelöste Speicherprobleme. Für weitere Informationen öffnen Sie Designer 4.0.2, und klicken Sie in der Symbolleiste auf *Help* > *What's New* (Hilfe > Neuigkeiten).
- **Designer-Optimierung für optionalen Import von Rollen und Ressourcen** Beim Konfigurieren eines Projekts in Designer war es bisher erforderlich, dass automatisch eine große Anzahl von Rollen und Ressourcen aus dem Identitätsdepot importiert werden musste. Jetzt kann Designer vom Benutzer so konfiguriert werden, dass der Rollenkatalog nicht mehr automatisch importiert werden soll. Wenn ein Benutzer nicht möchte, dass Rollen oder Ressourcen importiert werden, kann er die Option *Do not import role catalog (excluding system roles)* (Rollenkatalog nicht importieren (außer Systemrollen)) auf der Seite *Novell* > *Provisioning* > *Import/Deploy* (Novell > Provisioning > Importieren/Bereitstellen) in den Designer-Voreinstellungen deaktivieren. Der Rollenkatalog wird dann nicht automatisch in Designer importiert, wodurch die Benutzer Zeit sparen und diese Rollen und Ressourcen in Designer auch nicht verwalten müssen.

  Weitere Informationen finden Sie im Abschnitt „Configuring Roles“ (Konfigurieren von Rollen) im *User Application: Design Guide* (Benutzeranwendung: Entwurfshandbuch).
- **Entfernen nicht verwendeter Pakete aus dem Paketkatalog in Designer** Wenn ein Benutzer über eine große Anzahl nicht benötigter Pakete verfügt, die in den Paketkatalog importiert wurden, bietet Designer 4.0.2 die Möglichkeit an, nicht verwendete Pakete aus dem Katalog zu löschen. Dabei werden sämtliche importierten Pakete, die nicht in einem Treiber, Treibersatz oder Identitätsdepot installiert sind, aus dem Projekt entfernt.

  Weitere Informationen finden Sie im Abschnitt „Removing Packages from the Package Catalog“ (Entfernen von Paketen aus dem Paketkatalog) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Adminstrationshandbuch für Designer 4.0.2 for Identity Manager 4.0.2).

- **Analyzer-Funktionen:**
  - **Leistungsverbesserungen in Analyzer** Analyzer 4.0.2 bietet eine bessere Leistung durch Verwendung der Batching-Funktion beim MySQL-Datenbankserver. Analyzer kann jetzt eine Million Datensätze auf einmal in die Analyzer-Datenbank importieren. Weitere Informationen finden Sie unter „Database Settings“ (Datenbankeinstellungen) im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.2 für Identity Manager).

2.2 Funktionen von Identity Manager 4.0.1

- **Aktivität „Ressourcenanforderung“:** Die Aktivität „Ressourcenanforderung“ ermöglicht Ihnen, das Zuweisen bzw. Entziehen von Ressourcen zu automatisieren. Beispielsweise können Sie eine Bereitstellungsanforderungsdefinition schreiben, die einem neuen Mitarbeiter an seinem ersten Arbeitstag alle benötigten Ressourcen bereitstellt. Mithilfe der Aktivität „Ressourcenanforderung“ können Sie die Genehmigung von bestimmten Ressourcen für diesen

Mitarbeiter automatisieren. Ausführliche Informationen zur Aktivität „Ressourcenanforderung“ finden Sie unter „*Resource Request Activity*“ (Aktivität „Ressourcenanforderung“) im *User Application: Design Guide* (Designhandbuch zur Benutzeranwendung).

- **Telemetrie:** Identity Manager Telemetry ist ein neuer Auftrag, der in Identity Manager 4.0.1 eingeführt wurde. Der Auftrag kann als Zählprogramm für die Lizenznutzung und als Lizenzüberwachungswerkzeug eingesetzt werden. Mithilfe des Lizenzüberwachungswerkzeugs können Identity Manager-Kunden mehr Lizenzen hinzufügen oder nicht verwendete Lizenzen deaktivieren. Die Kunden können auch von Vorteilen wie z. B. der Preisgebung für inaktive Benutzer profitieren.

  Der Telemetrieauftrag sammelt Informationen zu den installierten Software- und Hardwarekomponenten von Identity Manager sowie zur Verwendung der Identity Manager-Treiber in der Kundenumgebung. Nachdem sich der Kunde beim Novell Customer Center registriert hat, werden die Informationen an Novell gesendet. Mithilfe der gesammelten Informationen kann Novell dem Kunden eine bessere Unterstützung bieten. Darüber hinaus wird Identity Manager effektiver und effizienter weiterentwickelt und getestet und es können wichtige Entscheidungen für zukünftige Versionen getroffen werden. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Jobs Guide* (Handbuch zu Identity Manager 4.0.1 Aufträgen).
- **Berichte:** Folgende Berichte wurden zum Identitätsberichterstellungsmodul hinzugefügt:
  - **Benutzerstatusänderung im Identitätsdepot:** Enthält für die Identitätsdepotbenutzer signifikante Ereignisse.
  - **Benutzerpasswortänderung im Identitätsdepot:** Zeigt alle Benutzerpasswortänderungen im Identitätsdepot an.
  - **Zugriffsanfragen nach Empfänger:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Empfänger.
  - **Zugriffsanfragen nach Anforderer:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Anforderer.
  - **Zugriffsanfragen nach Ressource:** Enthält die Workflow-Prozesse zu Ressourcenzuweisungen gruppiert nach Ressourcen.

2.3 Funktionen von Identity Manager 4.0

Neben den beschriebenen neuen Funktionen ist Identity Manager 4.0.1 mit den folgenden Funktionen ausgestattet, die in Identity Manager 4.0 hinzugefügt wurden.

- **Umfassende, sofort einsatzfähige Berichterstellung:** Mithilfe des integrierten Berichterstellungsmoduls von Novell Identity Manager 4.x lässt sich die Konformität von In-House- und Cloud-Bereitstellungen besser darstellen. Mit den Berichterstellungsfunktionen können Sie die Benutzerrechte und den Identitätsstatus eines bestimmten Benutzers anzeigen oder einen Bereitstellungsverlauf und einen Bericht über die vom Benutzer durchgeführten Aktionen erstellen. Weitere Informationen hierzu finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).
- **Erweiterte Integration:** Zum Erstellen einer neuen Identity Manager-Lösung, in der sich alle Komponenten auf demselben Server befinden, bietet Ihnen Novell Identity Manager 4.x ein integriertes Installationsprogramm, das die Installation erleichtert und mit dem Sie Ihr System schneller einrichten können. Anstatt die Identity Manager-Komponenten einzeln zu installieren, können Sie mithilfe des integrierten Installationsprogramms alle Komponenten in einem Installationsvorgang installieren. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).

- **Paketverwaltung:** Identity Manager 4.x bietet das neue Konzept „Paketverwaltung“. Dieses System dient zum Erstellen, Verteilen und Verwenden von hochwertigen Bausteinen mit Identity Manager-Richtlinieninhalten. Weitere Informationen zu Identity Manager-Paketen finden Sie unter *Configuring Packages* (Konfigurieren von Paketen) im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1).
- **Cloud-fähige Treiber:** Identity Manager 4.x bietet mehrere Treiber für die Integration in SaaS. Die Treiber lassen sich nahtlos in SaaS und die gehostete Lösung integrieren und bieten unter anderem folgende Funktionen: Bereitstellung, Deaktivierung der Bereitstellung, Anforderungs- bzw. Genehmigungsverfahren, Passwortänderungen, Identitätsprofilaktualisierungen und Berichterstellung. Mithilfe der Treiber „New SharePoint“ und „Salesforce.com“ können Sie Ihre Unternehmensidentitäten in Cloud-Anwendungen integrieren. Weitere Informationen zu cloud-fähigen Treibern finden Sie im *Identity Manager 4.0.2 Driver for Salesforce.com Implementation Guide* (Implementierungshandbuch für Identity Manager 4.0.2-Treiber für Salesforce.com) und im *Identity Manager 4.0.1 Driver for SharePoint Implementation Guide* (Implementierungshandbuch für Identity Manager 4.0.1-Treiber für SharePoint).
- **Eingebettetes Identitätsdepot:** Die Architektur von Novell Identity Manager 4.x umfasst ein optionales integriertes Identitätsdepot, wodurch das Erstellen und Verwalten einer separaten Verzeichnisstruktur für Identitätszwecke nicht mehr erforderlich ist. Zu den weiteren Ausstattungsmerkmalen der Novell Identity Manager 4.x-Produktfamilie gehören Treiber, die eine problemlose Integration des Identitätsdepots in andere Repositorys mit Identitätsinformationen, z. B. Active Directory oder verschiedene Datenbanken in Ihrem Unternehmen, ermöglichen. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).
- **Vereinfachte Identitäts- und Rollenverwaltung:** Die Novell Identity Manager 4.x-Produktfamilie vereinfacht die Integration von unterschiedlichen Rollen-Repositorys in einen konsolidierten Speicherort, sodass Sie nicht unterschiedliche Identifikationsinformationsquellen verwalten müssen. Über die neue intuitive Benutzeroberfläche des Rollenzuordnungsadministrators können Sie in Novell Identity Manager 4.x sogar Rollen und Profile von Drittanbietern zuordnen. Weitere Informationen hierzu finden Sie im *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* (Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 4.0.1).
- **Erweiterte Werkzeuge:** Designer ist ein wichtiges Werkzeug, das Ihnen umfassende Funktionen zum Entwerfen einer Identity Manager-Lösung bereitstellt, die auf Ihre Anforderungen zugeschnitten ist. In Designer 4.x wurden mehrere Funktionen verbessert bzw. erweitert. Welche Änderungen vorgenommen wurden, sehen Sie in der Liste unter *Neuheiten* (http://www.novell.com/documentation/designer401/resources/whatsnew/index.html). Weitere Informationen zu den Funktionen und der Verwaltung von Designer finden Sie im *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide* (Administrationshandbuch zu Designer 4.0.1 für Identity Manager 4.0.1). Darüber hinaus verfügt Identity Manager über ein Werkzeug, mit dem sich Daten einfacher analysieren und bereinigen lassen. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

3 Identity Manager-Familie

Die Identity Manager-Produktfamilie ist in drei Produktgruppen unterteilt, die auf die verschiedenen Kundenanforderungen zugeschnitten sind:

- Identity Manager Advanced Edition
- Identity Manager Standard Edition
- Compliance Management-Plattform

Die Identity Manager Advanced Edition enthält neben den Funktionen der Identity Manager Standard Edition noch zusätzliche Funktionen. Die Compliance Management-Plattform ist mit den Funktionen der Advanced und Standard Edition sowie zusätzlichen Werkzeugen ausgestattet.

Abbildung 3-1 *Identity Manager-Produktgruppen*

Eine Gegenüberstellung der Funktionen der Advanced und der Standard Edition von Identity Manager finden Sie im Versionenvergleich zu Identity Manager (http://www.novell.com/products/identitymanager/features/identitymanager-version-comparison.html).

- Abschnitt 3.1, „Identity Manager Advanced Edition“, auf Seite 24
- Abschnitt 3.2, „Identity Manager Standard Edition“, auf Seite 24

- Abschnitt 3.3, „Compliance Management-Plattform“, auf Seite 26
- Abschnitt 3.4, „Aktivieren der Standard und Advanced Edition von Identity Manager“, auf Seite 27

3.1 Identity Manager Advanced Edition

Die Identity Manager 4.0.2 Advanced Edition enthält einen vollständigen Satz an Funktionen zur Bereitstellung für Benutzer der Unternehmensklasse. Sie enthält die Identitätsselbstbedienungsfunktionen der Standard Edition sowie umfassende Funktionen für die Workflow-basierte Bereitstellung. Mithilfe der Advanced Edition können Sie Workflow-Genehmigungsverfahren initiieren sowie Rollen und Ressourcen bereitstellen und von den Vorteilen der Konformitätsfunktionen profitieren. Ein weiteres Ausstattungsmerkmal der Advanced Edition ist das Arbeits-Dashboard.

Identity Manager 4.0.2 Advanced Edition ist als separate ISO-Imagedatei erhältlich.

Hinweis: Außerdem ist eine 90-Tage-Testversion von Identity Manager 4.0.2 Advanced Edition verfügbar.

3.2 Identity Manager Standard Edition

Um die verschiedenen Kundenbedürfnisse zu erfüllen, hat Novell Identity Manager 4.0.2 Standard Edition auf den Markt gebracht. Die Standard Edition enthält einen Teil der Funktionen der Identity Manager Advanced Edition.

Die Standard Edition bietet auch weiterhin alle Funktionen, die in älteren Versionen von Identity Manager vorhanden sind:

- Identitätsynchronisierung
- Automatische regelbasierte Bereitstellung
- Passwortverwaltung und Passwortselbstbedienung
- Identitätsselbstbedienung mit vorhandenen White Pages und Organigrammfunktionen

---

Hinweis: Beide Identity Manager-Ausführungen (Advanced und Standard) enthalten weiterhin die gleichen Integrationsmodule.

Zusätzlich zu den oben aufgeführten Funktionen umfasst die Standard Edition die folgenden Funktionen der Advanced Edition:

- Erscheinungsbild der Benutzeroberfläche
- Berichterstellungsmodul
- Framework zum Verpacken von Inhalten
- Unterstützung für REST-APIs und Single Sign-on (SSO)
- Analyzer-Werkzeug für den Datenabgleich

Identity Manager 4.0.2 Standard Edition steht als separate ISO-Imagedatei zum Download zur Verfügung. Wenn Sie von der Standard Edition zur Advanced Edition aufrüsten möchten, verwenden Sie die Identity Manager Advanced Edition-ISO-Imagedatei. Sie müssen die richtige

Aktivierung anwenden, um auf die Advanced Edition aufrüsten zu können. Weitere Informationen zum Aufrüsten der Standard Edition auf die Advanced Edition finden Sie im *Identity Manager 4.0.2 Upgrade and Migration Guide* (Aufrüstungs- und Migrationshandbuch zu Identity Manager 4.0.1).

Es ist nicht möglich, von einer installierten Identity Manager Advanced Edition zur Standard Edition zu wechseln, indem Sie die ISO-Imagedatei der Standard Edition verwenden. Wenn Sie von der Identity Manager Advanced Edition zur Standard Edition wechseln möchten, deinstallieren Sie zunächst die Advanced Edition vom Server und installieren Sie dann die Standard Edition-ISO-Imagedatei vom Identity Manager-Medium.

Folgende Funktionen stehen in Identity Manager Standard Edition nicht zur Verfügung:

- Der Rollenzuordnungsadministrator ist nicht verfügbar.
- Folgende Beschränkungen gelten für die Benutzeranwendung:
  - **Geschäftsbenutzer haben nur Zugriff auf die Registerkarte „Identitätsselbstbedienung“:** Wenn Sie sich als Geschäftsbenutzer bei der Standard Edition von Identity Manager anmelden, wird in der Benutzeranwendung nur die Registerkarte *Identitätsselbstbedienung* angezeigt. Wenn Sie sich als Benutzeranwendungsadministrator anmelden, steht zudem die Registerkarte *Administration* zur Verfügung.
  - **Rollen und Ressourcen werden nicht unterstützt:** Die Verwendung von Rollen und Ressourcen ist nur in der Advanced Edition möglich. In der Standard Edition ist die Registerkarte *Rollen und Ressourcen* nicht verfügbar.
  - **Die Registerkarte „Konformität“ wird nicht unterstützt:** Die Registerkarte *Konformität* steht nur in Identity Manager 4.0.2 Advanced Edition zur Verfügung. In der Standard Edition ist die Registerkarte *Konformität* nicht verfügbar.
  - **Das Arbeits-Dashboard ist nicht verfügbar:** In der Standard Edition steht die Registerkarte *Arbeits-Dashboard* nicht zur Verfügung.
  - **Benutzerdefinierte Rollen werden nicht unterstützt:** Die Definition von benutzerdefinierten Rollen ist nicht möglich. Die Standard Edition unterstützt nur die Verwendung von Systemrollen.
  - **Workflows werden nicht unterstützt:** Das Initiieren von Genehmigungs-Workflows ist nicht möglich.
  - **REST-APIs:** Die REST-APIs, die sich auf Rollen, Ressourcen und Workflows beziehen, sind nicht für die Verwendung mit Identity Manager Standard Edition lizenziert. Die REST-APIs für Passwortselbstbedienung sind für die Verwendung mit der Standard Edition lizenziert.
  - **Vereinfachtes Sicherheitsmodell:** Die Standard Edition bietet ein vereinfachtes Sicherheitsmodell, mit dem die unbeabsichtigte Verwendung von Funktionen der Advanced Edition verhindert wird. Sie müssen nur die folgenden Administratorrollen zuweisen:
    - **Benutzeranwendungsadministrator:** Ein Benutzeranwendungsadministrator ist berechtigt, alle Verwaltungsfunktionen in Verbindung mit der Identity Manager-Benutzeranwendung auszuführen. Dies umfasst den Zugriff auf die Registerkarte *Administration* der Benutzeroberfläche von Identity Manager, um die dort verfügbaren Verwaltungsaktionen auszuführen.
    - **Berichtsadministrator:** Dieser Benutzer kann alle Funktionen in der Berichterstellungsdomäne verwenden. Der Berichtsadministrator kann für alle Objekte alle Aktionen innerhalb der Berichterstellungsdomäne durchführen.

- **Sicherheitsadministrator:** Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne. Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne durchführen. Da diese Rolle berechtigt ist, Benutzerzugriffe für alle Funktionen von Identity Manager Advanced Edition zu erteilen bzw. zu delegieren, wird sie von den Rollen Benutzeranwendungsverwaltung und Berichtsverwaltung getrennt behandelt.

Hinweis: Novell hat zu Testzwecken das Sicherheitsmodell in der Standard Edition nicht gesperrt. Der Sicherheitsadministrator kann daher alle Domänenadministratoren und beauftragte Administratoren sowie andere Sicherheitsadministratoren zuweisen. In der Produktionsumgebung werden diese erweiterten Funktionen jedoch nicht unterstützt, wie in der Endbenutzer-Lizenzvereinbarung beschrieben. In Produktionsumgebungen wird die Zuweisung der Administratoren durch die Lizenzierung beschränkt. Novell sammelt Überwachungsdaten in der Audit-Datenbank, um sicherzustellen, dass die Lizenzierung in der Produktionsumgebung eingehalten wird. Darüber hinaus ist es empfehlenswert, die Sicherheitsadministratorberechtigung nur einem Benutzer zu erteilen.

Weitere Informationen zum Einrichten der Benutzeranwendungsfunktionen finden Sie im *User Application: Administration Guide* (Benutzeranwendung: Administrationshandbuch).

- Folgende Beschränkungen gelten für das Identitätsberichterstellungsmodul:
  - **Treiber „Verwaltetes System - Gateway“ ist deaktiviert:** Der Treiber „Verwaltetes System – Gateway“ kann von jedem verwalteten System, das Berechtigungen unterstützt und in Identity Manager 4.0 oder neueren Versionen für die Datenerfassung aktiviert wurde, Informationen abrufen.

    Der Treiber „Verwaltetes System - Gateway“ ist in der Standard Edition von Identity Manager deaktiviert.
  - **Berichte enthalten nur Identitätsdepotinformationen:** Berichte, die mit Identity Manager Standard Edition generiert werden, enthalten nur Identitätsdepotdaten und keine Informationen zu verbundenen verwalteten Systemen.
  - **Berichte enthalten keine Verlaufsdaten:** In der Standard Edition ist es beim Erstellen von Berichten nicht möglich, Daten zum Statusverlauf abzurufen. Die Standard Edition gibt nur Daten wieder, die den aktuellen Status des Systems widerspiegeln.
  - **Einige Berichte sind nicht verfügbar:** In Identity Manager 4.0 und neueren Versionen wurden mehrere neue Berichte hinzugefügt. Die Standard Edition beinhaltet keine Berichte, die auf Daten zu verbundenen Systemen und historische Daten angewendet werden können.
  - **Einige Berichte enthalten keine Daten:** Einige Berichte sind nur für die Verwendung mit der Identity Manager Advanced Edition sinnvoll, da sie Daten beinhalten, die in der Standard Edition nicht verfügbar sind, z. B. Rollen, Ressourcen und Workflow-Prozesse.

3.3 Compliance Management-Plattform

Die Novell Compliance Management-Plattform kombiniert die Novell-Produkte zur Identitäts-, Zugriffs- und Sicherheitsverwaltung mit bewährten Werkzeugen, die eine einfache Implementierung und Verwaltung der Lösung ermöglichen. Die Plattform integriert Identitäts- und Zugriffsdaten in Sicherheitsdaten- und Ereignismanagement-Technologien und liefert so einen holistischen Echtzeitüberblick über alle Netzwerkereignisse im Unternehmen. Diese enge Integration liefert leistungsstarke Funktionen für das Risikomanagement und stellt sicher, dass die Geschäftspolitik automatisch in den IT-Alltag eingebunden wird. Weitere Informationen hierzu finden Sie auf der Website zur Compliance Management-Plattform (http://www.novell.com/documentation/ncmp10/).

3.4 Aktivieren der Standard und Advanced Edition von Identity Manager

Identity Manager Advanced Edition und Standard Edition müssen innerhalb von 90 Tagen nach der Installation aktiviert werden, anderenfalls wird ihre Funktion eingestellt. Die ISO-Imagedateien für Identity Manager Advanced Edition und Standard Edition funktionieren bis zu 90 Tage. Sie können Identity Manager-Produkte zu einem beliebigen Zeitpunkt während oder nach Ablauf der 90 Tage aktivieren. Weitere Informationen hierzu finden Sie unter „Aktivieren von Novell Identity Manager-Produkten“ im *Identity Manager 4.0.2 Framework Installationshandbuch*.

Wenn die Aktivierung der Standard Edition auf ein vorhandenes, nicht aktiviertes Advanced Edition-System angewendet wird, funktionieren der Metaverzeichnis-Server und die Treiber nicht mehr.

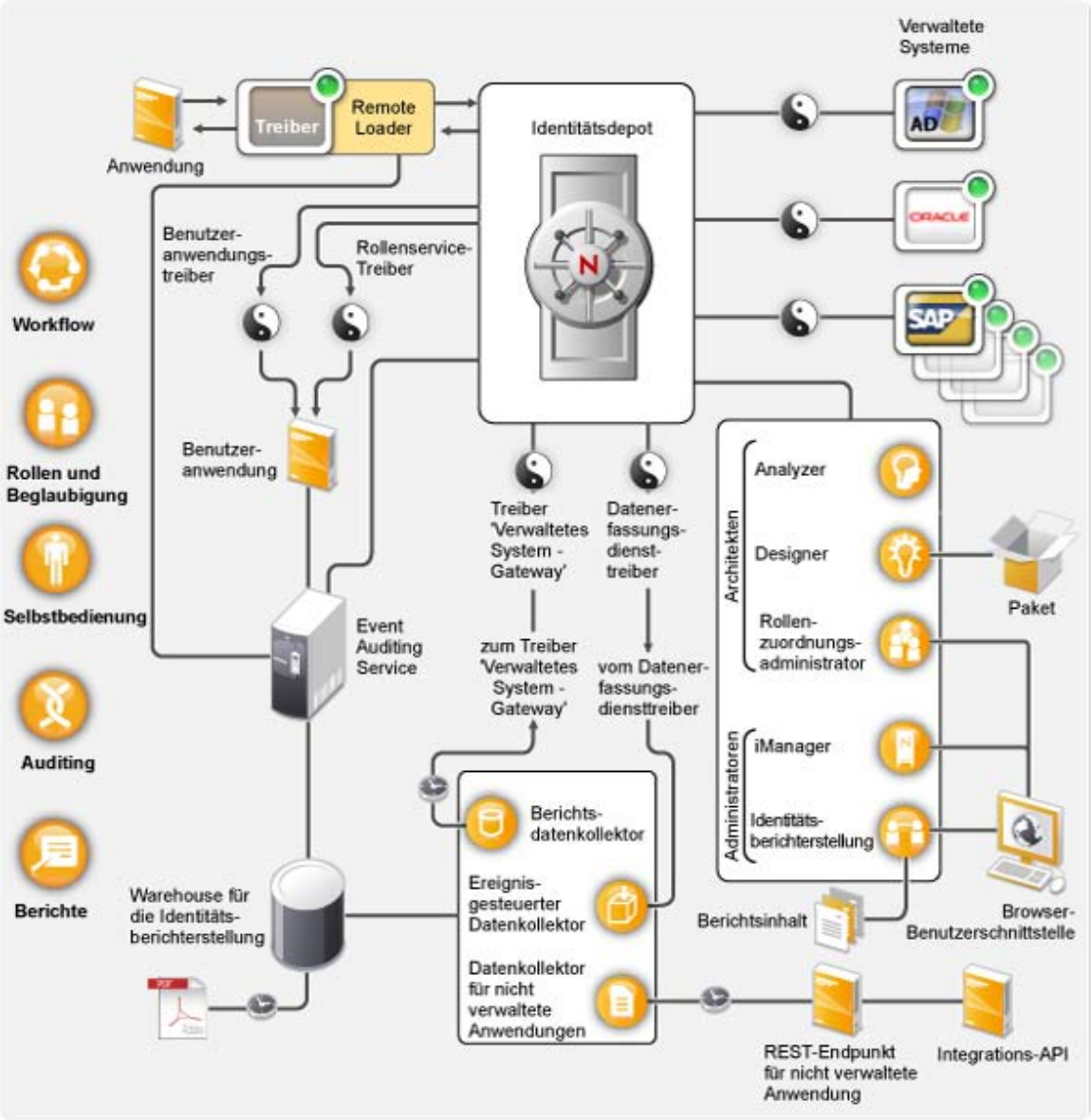
Hinweis: Wenn Sie sowohl Identity Manager Advanced Edition als auch Identity Manager Standard Edition verwenden, stellen Sie sicher, dass Sie die korrekte Aktivierung auf dem entsprechenden Server durchführen.

---

4 Identity Manager-Architektur

Das folgende Diagramm zeigt die High-Level-Architekturkomponenten für die Novell Identity Manager-Funktionen, die unter Kapitel 1, „Automatisierung von Geschäftsprozessen mit Identity Manager“, auf Seite 7 vorgestellt wurden: Datensynchronisierung, Workflow, Rollen, Beglaubigung, Selbstbedienung und Revision/Berichterstellung.

Abbildung 4-1 *High-Level-Architektur von Identity Manager*



Die einzelnen Komponenten werden in den folgenden Abschnitten erläutert:

- Abschnitt 4.1, „Datensynchronisierung“, auf Seite 30
- Abschnitt 4.2, „Workflow, Rollen, Beglaubigung und Selbstbedienung“, auf Seite 35
- Abschnitt 4.3, „Revision und Berichterstellung“, auf Seite 38

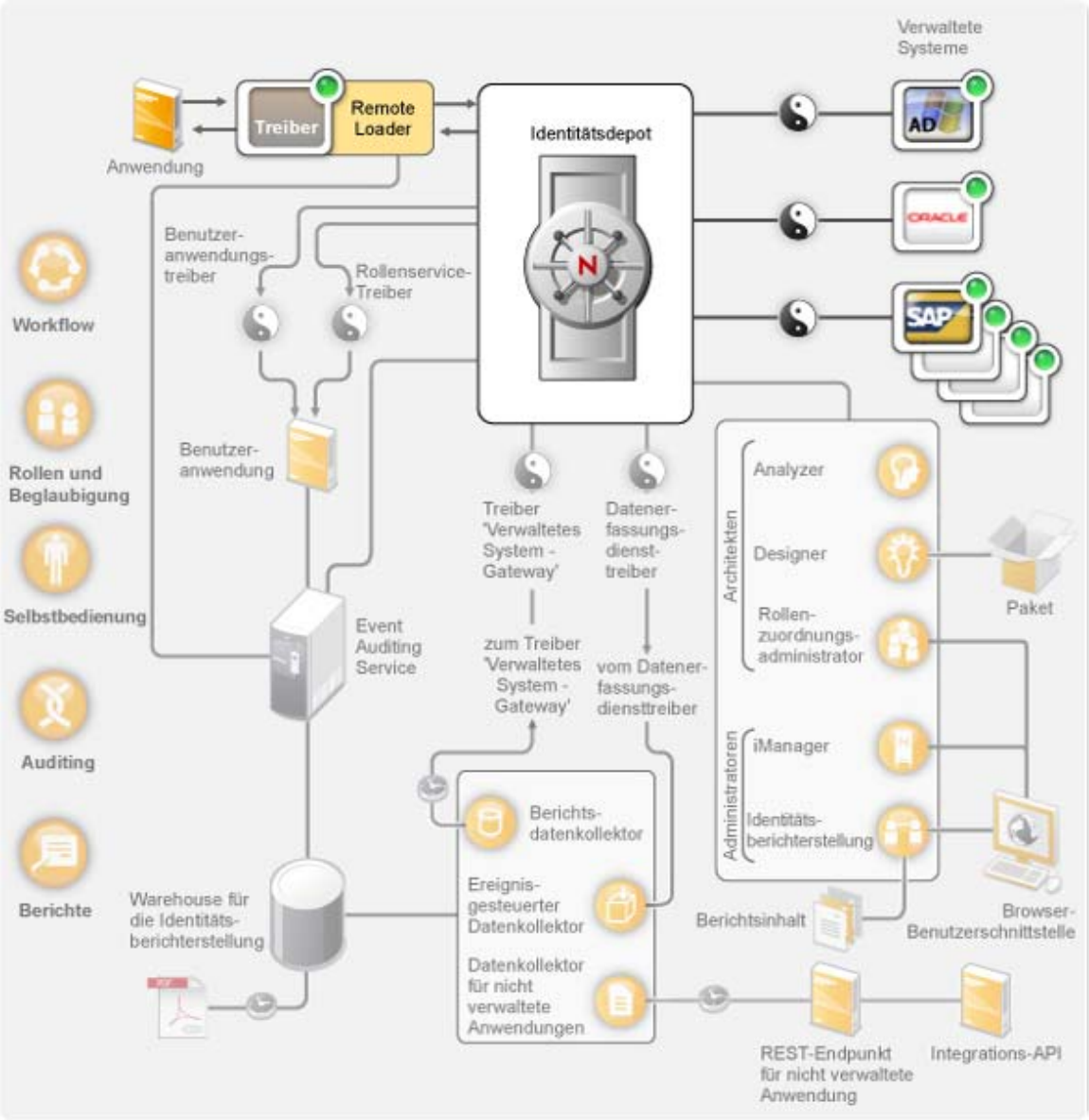
4.1 Datensynchronisierung

Die Datensynchronisierung bildet die Grundlage für die Automatisierung von Geschäftsprozessen. In ihrer einfachsten Form ist die Datensynchronisierung die Weitergabe von Daten von dem Speicherort, an dem ein Datenelement geändert wird, an andere Speicherorte, an denen es benötigt wird. Wenn beispielsweise die Telefonnummer eines Mitarbeiters im Personalsystem einer Firma geändert wird, wird die Änderung automatisch in allen anderen Systemen übernommen, in denen die Telefonnummer gespeichert ist.

Die Funktionen von Identity Manager gehen über die Synchronisierung von Identitätsdaten hinaus. Identity Manager kann alle Arten von Daten synchronisieren, die in der verbundenen Anwendung oder im Identitätsdepot gespeichert sind.

Die Datensynchronisierung wird einschließlich der Passwortsynchronisierung durch die fünf Basiskomponenten der Identity Manager-Lösung ermöglicht: das Identitätsdepot, die Identity Manager-Engine, die Treiber, der Remote Loader und die verbundenen Anwendungen. Diese Komponenten sind im folgenden Diagramm abgebildet.

Abbildung 4-2 *Identity Manager-Architekturkomponenten*



In den folgenden Abschnitten finden Sie Beschreibungen dieser Komponenten und Erläuterungen der Konzepte, die Sie verstehen sollten, um in Ihrer Organisation eine erfolgreiche Datensynchronisierung zwischen verschiedenen Systemen durchführen zu können:

- Abschnitt 4.1.1, „Komponenten“, auf Seite 31
- Abschnitt 4.1.2, „Wichtige Konzepte“, auf Seite 32

4.1.1 Komponenten

Identitätsdepot: Das Identitätsdepot dient als Metaverzeichnis der Daten, die zwischen Anwendungen synchronisiert werden sollen. Zum Beispiel werden Daten, die von einem PeopleSoft-System nach Lotus Notes synchronisiert werden, zuerst zum Identitätsdepot hinzugefügt, bevor sie

an das Lotus Notes-System gesendet werden. Außerdem werden im Identitätsdepot Identity Manager-spezifische Informationen gespeichert, z. B. Treiberkonfigurationen, Parameter und Richtlinien. Für das Identitätsdepot wird Novell eDirectory verwendet.

Identity Manager-Engine: Wenn im Identitätsdepot oder in einer verbundenen Anwendung Daten geändert werden, verarbeitet die Identity Manager-Engine die Änderungen. Bei Ereignissen, die im Identitätsdepot auftreten, verarbeitet die Engine die Änderungen und sendet über den Treiber Befehle an die Anwendung. Bei Ereignissen, die in der Anwendung auftreten, empfängt die Engine die Änderungen vom Treiber, verarbeitet diese und sendet Befehle an das Identitätsdepot. Die Identity Manager-Engine wird auch als Metaverzeichnis-Engine bezeichnet.

Treiber: Treiber stellen eine Verbindung zu den Anwendungen her, deren Identitätsinformationen Sie verwalten möchten. Ein Treiber hat zwei grundlegende Aufgaben: das Melden von Datenänderungen (Ereignissen) in der Anwendung an die Identity Manager-Engine sowie das Ausführen von Datenänderungen (Befehlen), die von der Identity Manager-Engine an die Anwendung gesendet werden.

Remote Loader: Die Treiber müssen auf demselben Server installiert und ausgeführt werden wie die Anwendung, zu der sie eine Verbindung herstellen. Wenn sich die Anwendung auf demselben Server wie die Identity Manager-Engine befindet, müssen Sie lediglich den Treiber auf diesem Server installieren. Befindet sich die Anwendung jedoch nicht auf demselben Server wie die Identity Manager-Engine (d. h. sie ist bezogen auf den Engine-Server remote, nicht lokal), müssen Sie den Treiber und den Remote Loader auf dem Server der Anwendung installieren. Der Remote Loader lädt den Treiber und kommuniziert an dessen Stelle mit der Identity Manager-Engine.

Anwendung: Ein System, ein Verzeichnis, eine Datenbank oder ein Betriebssystem, zu dem der Treiber eine Verbindung herstellt. Die Anwendung muss APIs enthalten, die ein Treiber zum Ermitteln und Ausführen von Anwendungsdatenänderungen verwenden kann. Anwendungen werden häufig als *verbundene Systeme* bezeichnet.

4.1.2 Wichtige Konzepte

Kanäle: Der Datenfluss zwischen dem Identitätsdepot und einem verbundenen System erfolgt durch zwei separate *Kanäle*. Der *Abonnentenkanal* ermöglicht den Datenfluss vom Identitätsdepot zu einem verbundenen System. Anders ausgedrückt, das verbundene System abonniert Daten aus dem Identitätsdepot. Der *Herausgeberkanal* ermöglicht den Datenfluss von einem verbundenen System zum Identitätsdepot. Anders ausgedrückt, das verbundene System veröffentlicht Daten im Identitätsdepot.

Darstellung von Daten: Daten fließen als *XML-Dokumente* durch einen Kanal. Ein XML-Dokument wird erstellt, wenn eine Änderung im Identitätsdepot oder im verbundenen System auftritt. Das XML-Dokument wird an die Identity Manager-Engine übergeben, die es mit den Filtern und Richtlinien verarbeitet, die dem Kanal des Treibers zugewiesen sind. Nachdem das XML-Dokument vollständig verarbeitet wurde, initiiert die Identity Manager-Engine mithilfe des Dokuments die entsprechenden Änderungen im Identitätsdepot (Herausgeberkanal) bzw. der Treiber initiiert die entsprechenden Änderungen im verbundenen System (Abonnentenkanal).

Datenmanipulation: Wenn ein XML-Dokument durch einen Treiberkanal fließt, wirken sich die dem Kanal zugewiesenen *Richtlinien* auf die Dokumentdaten aus.

Richtlinien werden für viele Zwecke eingesetzt, z. B. zum Ändern von Datenformaten, zum Zuordnen von Attributen zwischen dem Identitätsdepot und dem verbundenen System, zum bedingungsabhängigen Blockieren des Datenflusses, zum Generieren von Email-Benachrichtigungen und zum Bearbeiten des Datenänderungstyps.

Steuerung des Datenflusses: *Filter* bzw. *Filterrichtlinien* steuern den Datenfluss. Filter geben an, welche Datenelemente zwischen dem Identitätsdepot und einem verbundenen System synchronisiert werden. Zum Beispiel werden Benutzerdaten in der Regel zwischen Systemen synchronisiert. Deshalb sind die Benutzerdaten bei den meisten verbundenen Systemen im Filter aufgelistet. Drucker hingegen sind üblicherweise für die meisten Anwendungen nicht von Interesse, daher sind Druckerdaten bei den meisten verbundenen Systemen nicht im Filter aufgeführt.

Bei jeder Beziehung zwischen dem Identitätsdepot und einem verbundenen System sind zwei Filter vorhanden: ein Filter im Abonnentenkanal, der den Datenfluss vom Identitätsdepot zum verbundenen System steuert, und ein Filter im Herausgeberkanal, der den Datenfluss vom verbundenen System zum Identitätsdepot steuert.

Autorisierte Quellen: Die meisten identitätsbezogenen Datenelemente haben einen konzeptionellen Eigentümer. Der Eigentümer eines Datenelements wird als *autorisierte Quelle* für das Element angesehen. In der Regel darf nur die autorisierte Quelle eines Datenelements Änderungen an dem Datenelement vornehmen.

Zum Beispiel wird das Email-System eines Unternehmens im Allgemeinen als autorisierte Quelle für die Email-Adresse eines Mitarbeiters betrachtet. Wenn ein Administrator des White Pages-Verzeichnis des Unternehmens die Email-Adresse eines Mitarbeiters in diesem System ändert, hat die Änderung keine Auswirkung darauf, ob der Mitarbeiter tatsächlich an die geänderte Adresse gesendete Emails empfängt, da die Änderung im Email-System erfolgen muss, damit sie wirksam ist.

Identity Manager legt autorisierte Quellen für ein Element mithilfe von Filtern fest. Wenn beispielsweise der Filter für die Beziehung zwischen dem PBX-System und dem Identitätsdepot zulässt, dass die Telefonnummer eines Mitarbeiters vom PBX-System in das Identitätsdepot, jedoch nicht vom Identitätsdepot zum PBX-System fließt, ist das PBX-System die autorisierte Quelle für die Telefonnummer. Wenn alle anderen Beziehungen verbundener Systeme zulassen, dass die Telefonnummer vom Identitätsdepot zu den verbundenen Systemen fließt, jedoch nicht in die umgekehrte Richtung, bedeutet dies, dass das PBX-System die einzige autorisierte Quelle für Telefonnummern von Mitarbeitern im Unternehmen ist.

Automatisierte Bereitstellung: Automatisierte Bereitstellung bedeutet, dass Identity Manager neben der reinen Synchronisierung von Datenelementen auch andere Benutzerbereitstellungsaktionen generieren kann.

Zum Beispiel wird in einem typischen Identity Manager-System, bei dem die Personaldatenbank die autorisierte Quelle für die meisten Mitarbeiterdaten ist, durch das Hinzufügen eines Mitarbeiters zur Personaldatenbank die automatische Erstellung eines entsprechenden Kontos im Identitätsdepot veranlasst. Die Erstellung des Kontos im Identitätsdepot veranlasst wiederum die automatische Erstellung eines Email-Kontos für den Mitarbeiter im Email-System. Die zur Bereitstellung des Kontos im Email-System verwendeten Daten werden aus dem Identitätsdepot abgerufen und können den Namen des Mitarbeiters, den Standort, die Telefonnummer usw. umfassen.

Die automatische Bereitstellung von Konten, Zugriffsrechten und Daten kann auf verschiedene Weisen gesteuert werden:

- **Datenelementwerte:** Die automatische Erstellung eines Kontos in den Zugriffsdatenbanken für verschiedene Gebäude kann beispielsweise durch einen Wert im Standortattribut eines Mitarbeiters gesteuert werden.
- **Genehmigungsworkflows:** Die Erstellung eines Mitarbeiters in der Finanzabteilung kann beispielsweise eine automatische Email an den Abteilungsleiter mit der Anforderung einer Genehmigung für ein neues Mitarbeiterkonto im Finanzsystem veranlassen. Der

Abteilungsleiter wird über die Email auf eine Webseite geleitet, auf der er die Anforderung genehmigen oder ablehnen kann. Die Genehmigung kann dann die automatische Erstellung eines Kontos für den Mitarbeiter im Finanzsystem veranlassen.

- **Rollenzuweisungen:** Ein Mitarbeiter erhält beispielsweise die Rolle „Buchhalter“. Identity Manager stellt für den Mitarbeiter alle Konten, Zugriffsrechte und Daten bereit, die der Rolle „Buchhalter“ zugewiesen sind. Dies erfolgt über Systemworkflows (ohne menschliches Eingreifen), von Mitarbeitern durchgeführte Genehmigungsabläufe oder eine Kombination aus beidem.

Berechtigungen: Eine Berechtigung repräsentiert eine Ressource in einem verbundenen System, beispielsweise ein Konto oder eine Gruppenmitgliedschaft. Wenn ein Benutzer die Kriterien erfüllt, die für eine Berechtigung in einem verbundenen System festgelegt wurden, verarbeitet Identity Manager ein Ereignis für den Benutzer, mit dem Ergebnis, dass dem Benutzer Zugriff auf die Ressource gewährt wird. Dies erfordert natürlich, dass alle Richtlinien wirksam sind, damit der Zugriff auf die Ressource möglich ist. Wenn zum Beispiel ein Benutzer die Kriterien für ein Exchange-Konto in Active Directory erfüllt, verarbeitet die Identity Manager-Engine den Benutzer mithilfe der Active Directory-Treiberrichtlinien, die ein Exchange-Konto bereitstellen.

Der Hauptnutzen von Berechtigungen besteht darin, dass Sie die Geschäftslogik für den Zugriff auf eine Ressource in einer Berechtigung statt in mehreren Treiberrichtlinien definieren können. Zum Beispiel können Sie eine Kontoberechtigung definieren, die einem Benutzer in vier verbundenen Systemen ein Konto zur Verfügung stellt. Die Entscheidung, ob für den Benutzer ein Konto bereitgestellt werden soll, wird durch die Berechtigung getroffen, was bedeutet, dass die Richtlinien für die einzelnen vier Treiber die Geschäftslogik nicht enthalten müssen. Stattdessen müssen die Richtlinien nur den Mechanismus für die Gewährung des Kontos liefern. Wenn Sie eine Änderung an der Geschäftslogik vornehmen müssen, führen Sie dies in der Berechtigung aus und nicht in den einzelnen Treibern.

Aufträge: Die meisten Aktionen, die Identity Manager ausführt, erfolgen als Reaktion auf Datenänderungen oder Benutzeranforderungen. Wenn beispielsweise Daten in einem System geändert werden, ändert Identity Manager die entsprechenden Daten in einem anderen System. Wenn ein Benutzer Zugriff auf ein System anfordert, initiiert Identity Manager die entsprechenden Prozesse (Workflows, Ressourcenbereitstellung usw.) für die Gewährung des Zugriffs.

Aufträge ermöglichen Identity Manager das Ausführen von Aktionen, die nicht durch Datenänderungen oder Benutzeranforderungen initiiert werden. Ein Auftrag besteht aus Konfigurationsdaten, die im Identitätsdepot gespeichert sind, und einem entsprechenden Implementierungscode. Identity Manager enthält vordefinierte Aufträge, die Aktionen wie das Starten oder Anhalten von Treibern, das Senden von Email-Benachrichtigungen über ablaufende Passwörter und das Prüfen des Zustands von Treibern ausführen. Sie können auch benutzerdefinierte Aufträge zur Durchführung weiterer Aktionen implementieren. Für einen benutzerdefinierten Auftrag müssen Sie (bzw. ein Entwickler oder Berater) den für die Durchführung der gewünschten Aktionen erforderlichen Code erstellen.

Aufträge: In der Regel werden Änderungen an Daten im Identitätsdepot oder in einer verbundenen Anwendung sofort verarbeitet. Mithilfe von Aufträgen können Sie Aufgaben planen, die an einem bestimmten Datum und zu einer bestimmten Uhrzeit ausgeführt werden sollen. Zum Beispiel wird ein neuer Mitarbeiter eingestellt, der jedoch erst im nächsten Monat bei dem Unternehmen anfängt. Der Mitarbeiter muss zur Personaldatenbank hinzugefügt werden, er soll jedoch erst ab seinem ersten Arbeitstag Zugriff auf die Ressourcen des Unternehmens (Email, Server usw.) erhalten. Ohne die Verwendung eines Auftrags würde der Benutzer den Zugriff sofort erhalten. Wenn Aufträge implementiert sind, wird ein Auftrag erstellt, der die Kontobereitstellung erst am ersten Arbeitstag des Mitarbeiters initiiert.

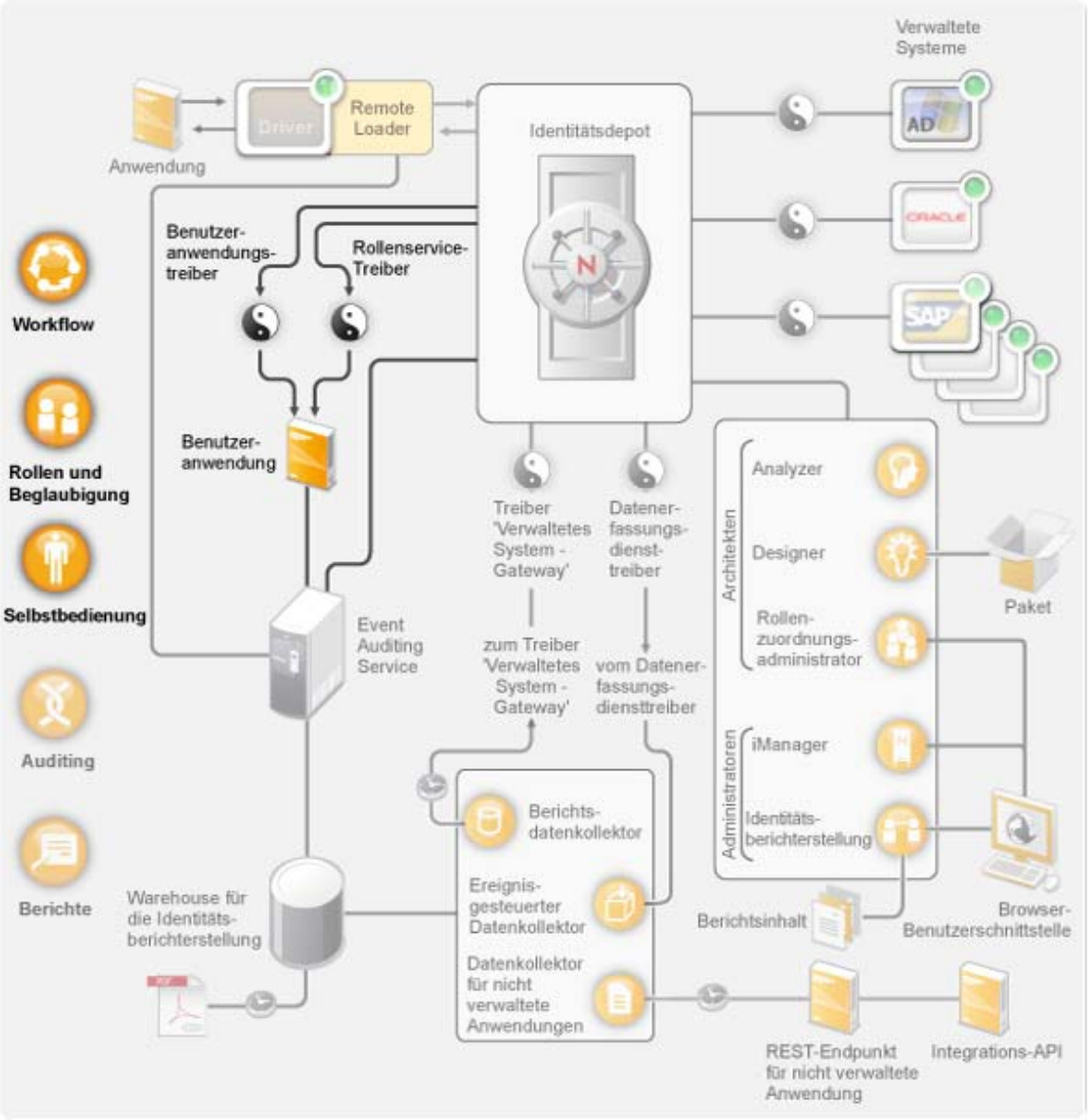
4.2 Workflow, Rollen, Beglaubigung und Selbstbedienung

Identity Manager bietet eine spezialisierte Anwendung, die Benutzeranwendung, die Genehmigungsworkflows, Rollenzuweisungen, die Beglaubigung und die Identitätsselbstbedienung ermöglicht.

Die Standard-Benutzeranwendung ist in Identity Manager enthalten. Die Standardversion bietet die Passwortselbstbedienung, mit deren Hilfe Benutzer vergessene Passwörter wiedererlangen oder zurücksetzen können, Organigramme für die Verwaltung von Benutzerverzeichnisinformationen, Benutzerverwaltungsfunktionen, die das Erstellen von Benutzern im Identitätsdepot ermöglichen, sowie Grundfunktionen der Identitätsselbstbedienung wie das Verwalten von Benutzerprofilinformationen.

Das rollenbasierte Bereitstellungsmodul der Benutzeranwendung ist eine Komponente von Identity Manager 4.0.2 Advanced Edition. Mit dem rollenbasierten Bereitstellungsmodul stehen Ihnen neben den Funktionen der Standard-Benutzeranwendung die erweiterte Selbstbedienung, der Genehmigungsworkflow, die rollenbasierte Bereitstellung, Funktionstrennungsbeschränkungen und die Beglaubigung zur Verfügung. Identity Manager 4.0.2 Advanced Edition umfasst die Standardfunktionen und die Funktionen des rollenbasierten Bereitstellungsmoduls.

Abbildung 4-3 *Identity Manager-Benutzeranwendung*



In den folgenden Abschnitten finden Sie Beschreibungen dieser Komponenten sowie Erläuterungen der Konzepte, die Sie verstehen sollten, um die Komponenten erfolgreich implementieren und verwalten zu können:

- Abschnitt 4.2.1, „Komponenten“, auf Seite 36
- Abschnitt 4.2.2, „Wichtige Konzepte“, auf Seite 37

4.2.1 Komponenten

Benutzeranwendung: Die Benutzeranwendung ist eine browserbasierte Webanwendung, die Benutzern und Geschäftsadministratoren die Möglichkeit bietet, verschiedene Identitätsselbstbedienungs- und Rollenbereitstellungsaufgaben auszuführen, z. B. das Verwalten von Passwörtern und Identitätsdaten, das Initiieren und Überwachen von Bereitstellungs- und Rollenzuweisungsanforderungen, das Verwalten des Genehmigungsverfahrens für

Bereitstellungsanforderungen und das Prüfen von Beglaubigungsberichten. Sie beinhaltet die Workflow-Engine, die die Weiterleitung von Anforderungen im Rahmen des entsprechenden Genehmigungsverfahrens steuert.

Benutzeranwendungstreiber: Der Benutzeranwendungstreiber speichert Konfigurationsinformationen und benachrichtigt die Benutzeranwendung über Änderungen im Identitätsdepot. Er kann darüber hinaus so konfiguriert werden, dass er das Auslösen von Workflows durch Ereignisse zulässt, und dass er der Benutzeranwendung den Erfolg oder das Fehlschlagen der Bereitstellungsaktivität eines Workflows meldet, sodass Benutzer den endgültigen Status ihrer Anforderungen sehen können.

Rollen- und Ressourcenservice-Treiber: Der Rollen- und Ressourcenservice-Treiber verwaltet alle Rollen- und Ressourcenzuweisungen, startet Workflows für Rollen- und Ressourcenzuweisungsanforderungen, die eine Genehmigung erfordern, und verwaltet indirekte Rollenzuweisungen nach Gruppen- und Containermitgliedschaften. Der Treiber erteilt und entzieht Berechtigungen für Benutzer basierend auf ihren Rollenmitgliedschaften und führt Bereinigungsprozeduren für abgeschlossene Anforderungen durch.

4.2.2 Wichtige Konzepte

Workflow-basierte Bereitstellung: Die Workflow-basierte Bereitstellung bietet den Benutzern die Möglichkeit, Zugriff auf Ressourcen anzufordern. Eine Bereitstellungsanforderung wird durch einen vordefinierten Workflow weitergeleitet, der möglicherweise die Genehmigung durch eine oder mehrere Personen beinhaltet. Wenn alle Genehmigungen erteilt wurden, erhält der Benutzer Zugriff auf die Ressource. Bereitstellungsanforderungen können auch indirekt als Reaktion auf Ereignisse im Identitätsdepot initiiert werden. Zum Beispiel kann durch das Hinzufügen eines Benutzers zu einer Gruppe eine Anforderung für die Erteilung des Zugriffs auf eine bestimmte Ressource für den Benutzer initiiert werden.

Rollenbasierte Bereitstellung: Die rollenbasierte Bereitstellung ermöglicht, dass Benutzer auf der Grundlage der ihnen zugewiesenen Rollen Zugriff auf bestimmte Ressourcen erhalten. Benutzern können eine oder mehrere Rollen zugewiesen werden. Wenn eine Rollenzuweisung eine Genehmigung erfordert, startet die Zuweisungsanforderung einen Workflow.

Funktionstrennung: Damit Benutzern keine widersprüchlichen Rollen zugewiesen werden, bietet das rollenbasierte Bereitstellungsmodul der Benutzeranwendung die Möglichkeit der Funktionstrennung. Sie können Funktionstrennungsbeschränkungen einrichten, die definieren, welche Rollen als widersprüchlich zueinander angesehen werden. Wenn Rollen im Widerspruch zueinander stehen, haben Funktionstrennungsgenehmiger die Möglichkeit, Ausnahmen von den Beschränkungen zu genehmigen oder zu verweigern. Genehmigte Ausnahmen werden als Funktionstrennungsverletzungen aufgezeichnet und können mithilfe des nachfolgend beschriebenen Beglaubigungsprozesses überprüft werden.

Rollenverwaltung: Die Rollen müssen von Mitarbeitern verwaltet werden, denen die Systemfunktionen Rollenmodul-Administrator und Rollenmanager zugewiesen wurden.

Der Rollenmodul-Administrator kann neue Rollen erstellen, vorhandene Rollen ändern, Rollen entfernen, Beziehungen zwischen Rollen ändern, Rollenzuweisungen für Benutzer erteilen und entziehen sowie Funktionstrennungsbeschränkungen erstellen, ändern und entfernen.

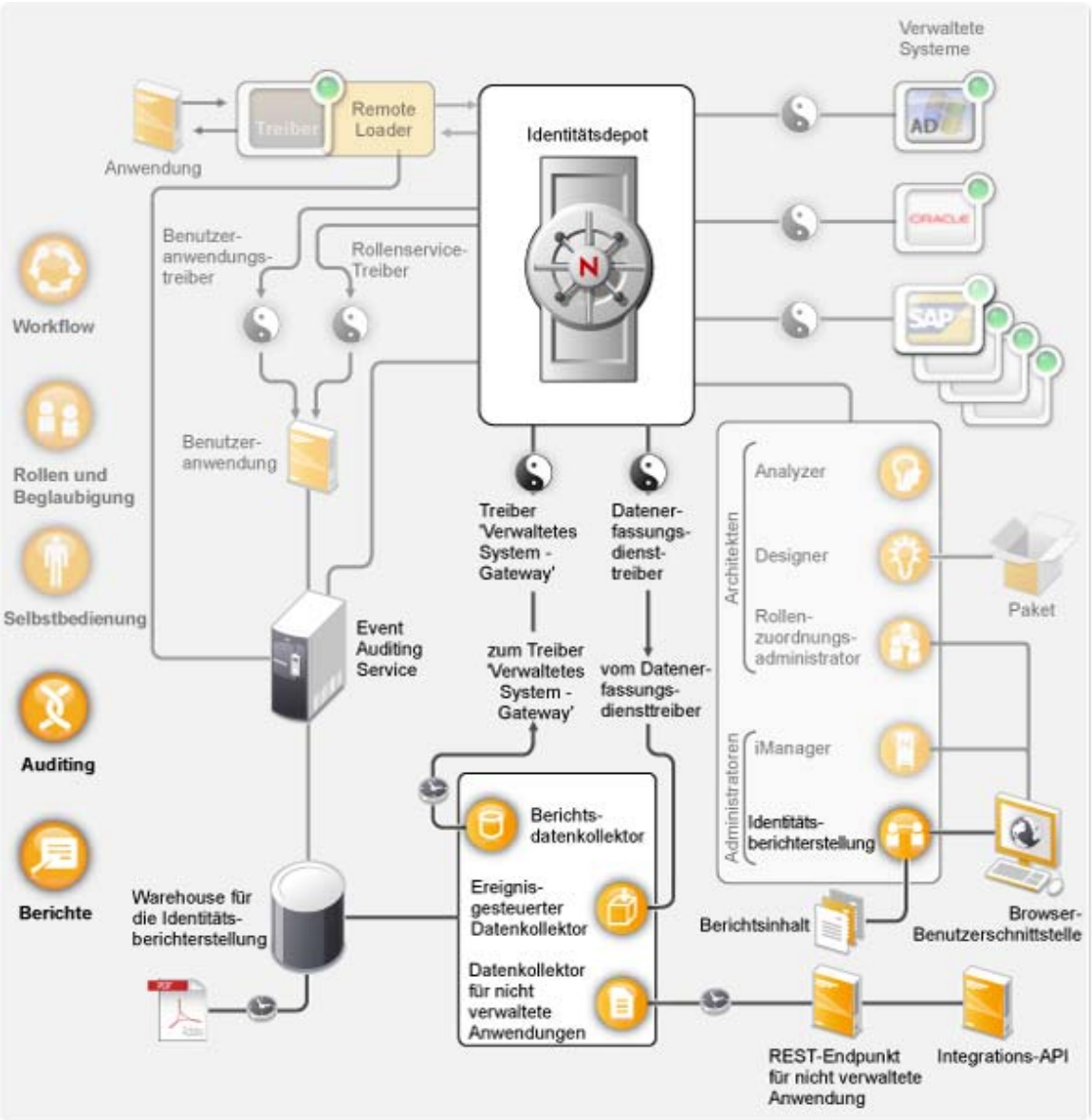
Der Rollenmanager kann dieselben Aufgaben durchführen wie der Rollenmodul-Administrator, mit Ausnahme des Verwaltens von Funktionstrennungsbeschränkungen, der Konfiguration des Rollensystems und des Ausführens aller Berichte. Außerdem bestehen für den Rollenmodul-Administrator keine Bereichsbeschränkungen innerhalb des Rollensystems, während der Bereich des Rollenmanagers auf speziell ausgewiesene Benutzer, Gruppen und Rollen beschränkt ist.

Beglaubigung: Rollenzuweisungen bestimmen den Zugriff eines Benutzers auf Ressourcen innerhalb Ihrer Organisation. Falsche Zuweisungen können die Einhaltung von Unternehmens- und behördlichen Bestimmungen gefährden. Mit Identity Manager können Sie die Richtigkeit von Rollenzuweisungen durch einen Beglaubigungsprozess validieren. Dieser Prozess ermöglicht einzelnen Benutzern das Überprüfen ihrer eigenen Profilinformationen und Rollenmanagern die Validierung von Rollenzuweisungen und Funktionstrennungsverletzungen.

4.3 Revision und Berichterstellung

Revision und Berichterstellung stehen über das Identitätsberichterstellungsmodul, eine neue Funktion von Identity Manager 4.0.2, zur Verfügung (siehe nachfolgendes Diagramm).

Abbildung 4-4 *Revision und Berichterstellung in Identity Manager*



Mit dem Identitätsberichterstellungsmodul können Sie Berichte generieren, die unternehmenskritische Informationen zu verschiedenen Aspekten Ihrer Identity Manager-Konfiguration liefern, einschließlich erfasster Informationen zu Identitätsdepots oder verwalteten Systemen, z. B. Active Directory oder SAP. Das Identitätsberichterstellungsmodul verwaltet die Daten mittels folgender Komponenten:

Event Auditing Service: Dieser Dienst protokolliert Aktionen, die im Berichterstellungsmodul durchgeführt wurden, z. B. das Importieren, Ändern, Löschen oder Planen eines Berichts. Der Event Auditing Service (EAS) protokolliert Aktionen, die im rollenbasierten Bereitstellungsmodul und im Rollenzuordnungsadministrator durchgeführt wurden.

Identitätsinformations-Warehouse: Repository für folgende Informationen:

- Berichtverwaltungsinformationen, z. B. Berichtsdefinitionen, Berichtzeitpläne und abgeschlossene Berichte, für die Berichterstellung verwendete Datenbankansichten und Konfigurationsinformationen.
- Identifikationsdaten, die vom Berichtsdatenkollektor, vom ereignisgesteuerten Datenkollektor und vom Datenkollektor für nicht verwaltete Anwendungen gesammelt wurden.
- Revisionsdaten mit Ereignissen, die vom Event Auditing Service erfasst wurden.

Die Daten des Identitätsinformations-Warehouses werden in der SIEM-Datenbank (Security Information and Event Management) gespeichert.

Datenerfassungsdienst: Ein Dienst, der Informationen von verschiedenen Quellen innerhalb der Organisation sammelt. Der Datenerfassungsdienst ist in drei Unterdienste unterteilt:

- **Berichtsdatenkollektor:** Verwendet ein Pull-Modell zum Abrufen von Daten aus einer oder mehreren Identitätsdepot-Datenquellen. Die Sammlung der Daten wird regelmäßig auf Grundlage der festgelegten Konfigurationsparameter durchgeführt. Der Kollektor ruft zum Abrufen der Daten den Treiber „Verwaltetes System - Gateway“ auf.
- **Ereignisgesteuerter Datenkollektor:** Verwendet ein Push-Modell zum Sammeln von Ereignisdaten, die vom Datenerfassungsdiensttreiber erfasst wurden.
- **Datenkollektor für nicht verwaltete Anwendungen:** Ruft Daten von einer oder mehreren nicht verwalteten Anwendungen ab, indem er einen speziell für jede Anwendung geschriebenen REST-Endpunkt aufruft. Nicht verwaltete Anwendungen sind Anwendungen in Ihrem Unternehmen, die nicht mit dem Identitätsdepot verbunden sind. Weitere Informationen hierzu finden Sie unter „REST Services for Reporting“ (REST-Dienste für Berichterstellung) im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

Datenerfassungsdiensttreiber: Ein Treiber, der Änderungen an Objekten im Identitätsdepot erfasst, z. B. Konten, Rollen, Ressourcen, Gruppen und Teammitgliedschaften. Der Datenerfassungsdiensttreiber registriert sich beim Datenerfassungsdienst und gibt Änderungsereignisse (z. B. Datensynchronisierung sowie Hinzufügen, Ändern und Löschen von Ereignissen) an den Datenerfassungsdienst weiter.

Änderungen an folgenden Objekten werden aufgezeichnet:

- Benutzerkonten und Identitäten
- Rollen und Rollenebenen
- Gruppen

Hinweis: Dynamische Gruppen werden vom Berichterstellungsmodul nicht unterstützt. Es werden nur Berichte von statischen Gruppen generiert.

- Gruppenmitgliedschaften
- Bereitstellungsanforderungsdefinitionen
- Funktionstrennungsdefinitionen und -verletzungen
- Benutzerberechtigungsverknüpfungen
- Ressourcendefinitionen und Ressourcenparameter
- Rollen- und Ressourcenzuweisungen
- Identitätsdepotberechtigungen, Berechtigungstypen und Treiber

Treiber „Verwaltetes System - Gateway“ Dieser Treiber sammelt Daten von verwalteten Systemen. Der Treiber führt zum Abrufen der Daten der verwalteten Systeme eine Identitätsdepotabfrage durch. Folgende Daten werden abgerufen:

- Liste aller verwalteten Systeme
- Liste mit allen Konten für die verwalteten Systeme
- Berechtigungstypen, Werte und Zuweisungen sowie Benutzerkontenprofile für die verwalteten Systeme

Identitätsberichterstellung: Über die Benutzeroberfläche des Berichterstellungsmoduls können Sie problemlos festlegen, dass die Berichtgenerierung außerhalb der Hauptgeschäftszeit ausgeführt und somit die Systemleistung nicht beeinträchtigt wird. Weitere Informationen hierzu finden Sie im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

Berichte: Identity Manager enthält vordefinierte Berichte, um die Daten im Identitätsinformations-Warehouse sinnvoll darzustellen. Sie können auch benutzerdefinierte Berichte erstellen. Weitere Informationen zu den Berichten finden Sie unter *Verwenden von Identity Manager 4.0.2 Berichten*. Weitere Informationen zu benutzerdefinierten Berichten finden Sie unter „Creating Custom Report Definitions“ (Erstellen von benutzerdefinierten Berichtsdefinitionen) im *Identity Reporting Module Guide* (Handbuch zum Identitätsberichterstellungsmodul).

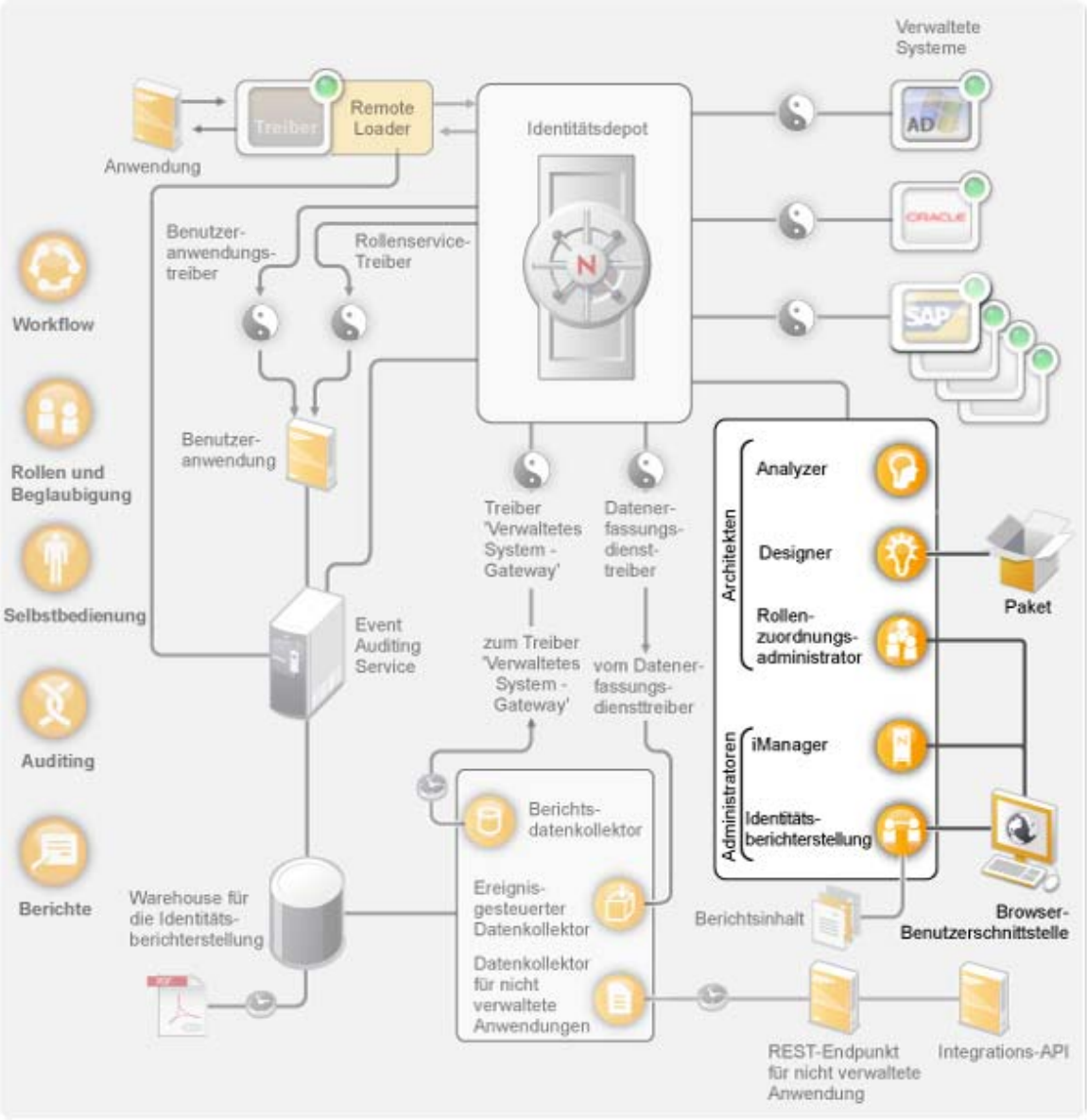
REST-Endpunkt für nicht verwaltete Anwendung: Eine nicht verwaltete Anwendung ist eine Anwendung, die nicht mit dem Identitätsdepot verbunden ist, jedoch Daten enthält, die im Bericht aufgezeichnet werden sollen. Wenn Sie einen REST-Endpunkt für die Anwendung festlegen, kann das Berichterstellungsmodul Daten aus der Anwendung abrufen.

Integrations-API: Das Identitätsberichterstellungsmodul bietet mehrere REST-APIs, mit denen Sie REST-Endpunkte für nicht verwaltete Anwendungen festlegen sowie benutzerdefinierte Anwendungen für die Berichterstellung schreiben können.

5 Identity Manager-Werkzeuge

Identity Manager stellt Ihnen Werkzeuge zum Erstellen und Verwalten Ihrer Identity Manager-Lösung zur Verfügung. Mit jedem Werkzeug werden spezifische Funktionen ausgeführt.

Abbildung 5-1 *Identity Manager-Werkzeuge*



Mithilfe von Designer können Sie Ihr Identity Manager-System in einer Offline-Umgebung entwerfen, erstellen und konfigurieren und Ihre Änderungen dann in Ihr Live-System übertragen. Darüber hinaus bietet Designer Paketverwaltungsfunktionen zum Vorkonfigurieren und Anpassen der Identity Manager-Treiberrichtlinien. Analyzer wird beim Erstellen der Identity Manager-Lösung zur Datenanalyse und -bereinigung sowie zur Vorbereitung der Datensynchronisierung verwendet.

Der Rollenzuordnungsadministrator dient zum Erstellen und Verwalten von Rollen in Ihrer Identity Manager-Lösung.

Mit iManager können Sie die gleichen Aufgaben wie mit Designer durchführen und zudem den Zustand Ihres Systems überwachen. Die Paketverwaltung wird in iManager jedoch nicht unterstützt. Es ist empfehlenswert, iManager für Verwaltungsaufgaben und Designer für Konfigurationsaufgaben, die Änderungen an Paketen, Modellierung und Tests vor der Bereitstellung erfordern, zu verwenden.

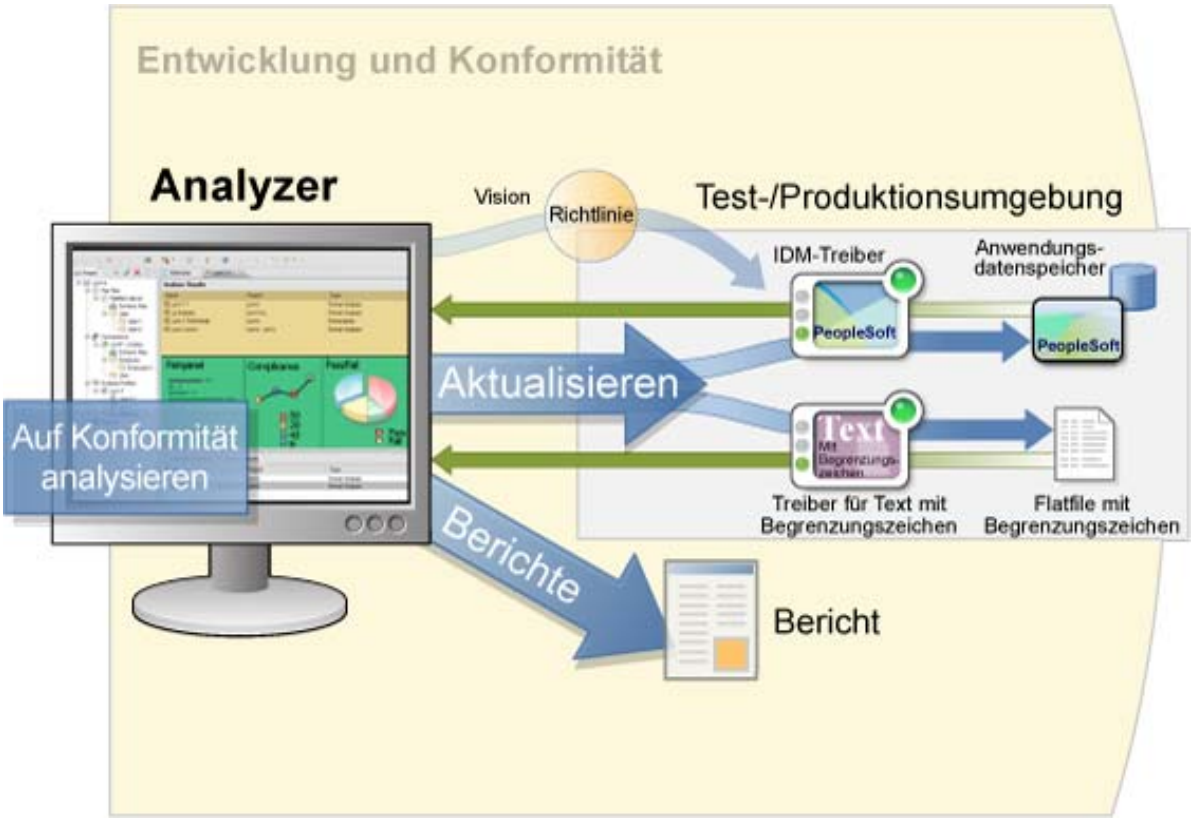
In den folgenden Abschnitten finden Sie weitere Informationen zu den einzelnen Werkzeugen:

- Abschnitt 5.1, „Analyzer“, auf Seite 42
- Abschnitt 5.2, „Designer“, auf Seite 43
- Abschnitt 5.3, „iManager“, auf Seite 45
- Abschnitt 5.4, „Rollenzuordnungsadministrator“, auf Seite 45
- Abschnitt 5.5, „Identitätsberichterstellung“, auf Seite 46

5.1 Analyzer

Analyzer ist ein Eclipse-basierter Satz von Identitätsverwaltungswerkzeugen, der Ihnen hilft, sicherzustellen, dass mithilfe der Datenanalyse und Datenbereinigung sowie des Datenabgleichs, der Datenüberwachung und der Datenberichterstellung interne Datenqualitätsrichtlinien eingehalten werden. Mit Analyzer können Sie alle Datenspeicher des Unternehmens analysieren, verbessern und kontrollieren.

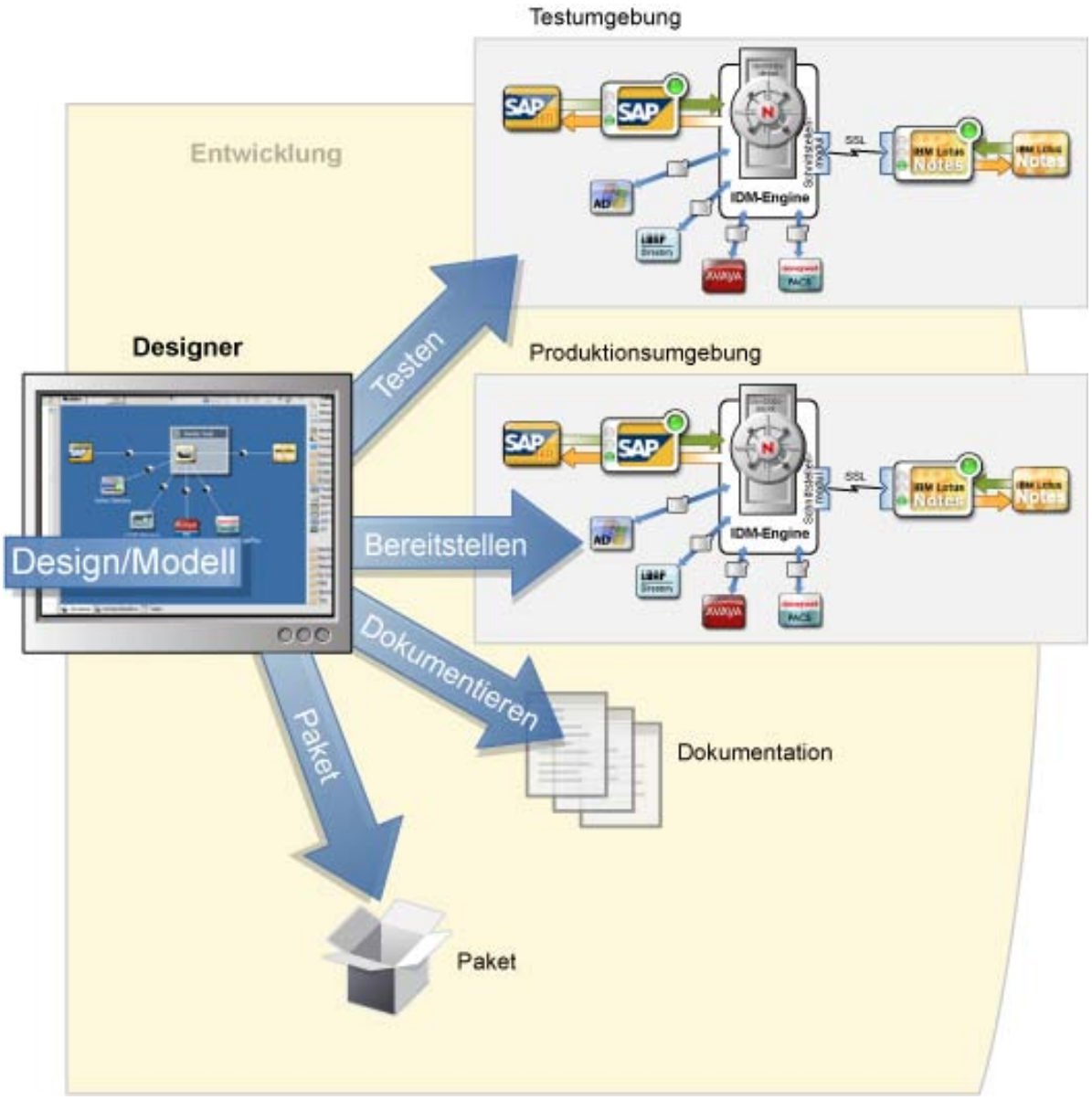
Abbildung 5-2 *Analyzer für Identity Manager*



5.2 Designer

Designer ist ein Eclipse-basiertes Werkzeug, mit dessen Hilfe Sie das Identity Manager-System entwerfen, bereitstellen und dokumentieren können. Mit der grafischen Schnittstelle von Designer können Sie Ihr System in einer Offline-Umgebung entwerfen und testen, das System in Ihrer Produktionsumgebung bereitstellen und alle Details Ihres bereitgestellten Systems dokumentieren.

Abbildung 5-3 *Designer für Identity Manager*



Entwerfen: Designer bietet eine grafische Schnittstelle, über die Sie Ihr System modellieren können. Dabei stehen Ansichten zur Verfügung, in denen Sie die Verbindungen zwischen Identity Manager und Anwendungen erstellen und steuern, Richtlinien konfigurieren und den Datenfluss zwischen verbundenen Anwendungen manipulieren können.

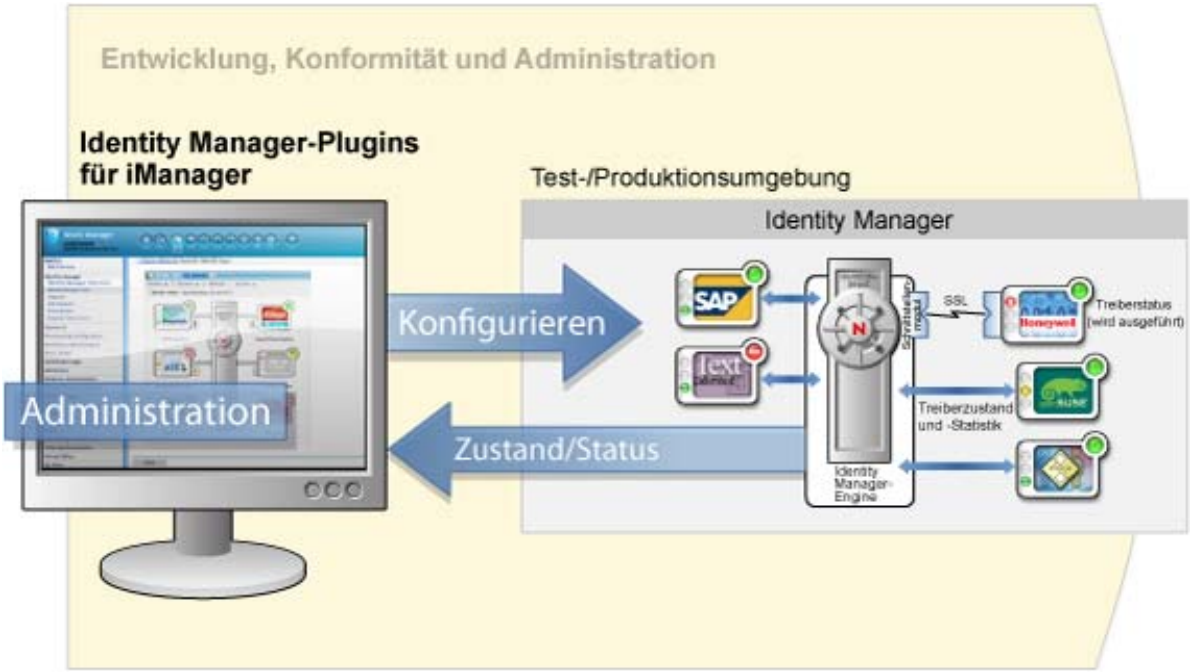
Bereitstellen: Ihre in Designer ausgeführte Arbeit wird erst dann in Ihrer Produktionsumgebung bereitgestellt, wenn Sie die Bereitstellung initiieren. Dadurch besitzen Sie die Freiheit, zu experimentieren, die Ergebnisse zu testen und Probleme zu beheben, bevor das System in Ihrer Produktionsumgebung eingesetzt wird.

Dokument: Sie können umfangreiche eine Dokumentation generieren, die Ihre Systemhierarchie, Treiberkonfigurationen, Richtlinienkonfigurationen und vieles mehr darstellt. Sie erhalten dadurch alle Informationen, die zum Verständnis der technischen Aspekte Ihres Systems erforderlich sind, und die Überprüfung der Konformität mit Ihren geschäftlichen Regeln und Richtlinien wird vereinfacht.

5.3 iManager

Novell iManager ist ein browserbasiertes Werkzeug, das einen einzelnen Administrationspunkt für viele Novell-Produkte, einschließlich Identity Manager, zur Verfügung stellt. Mithilfe der Identity Manager-Plugins für iManager können Sie Identity Manager verwalten und Echtzeitinformationen zum Zustand und Status Ihres Identity Manager-Systems erhalten.

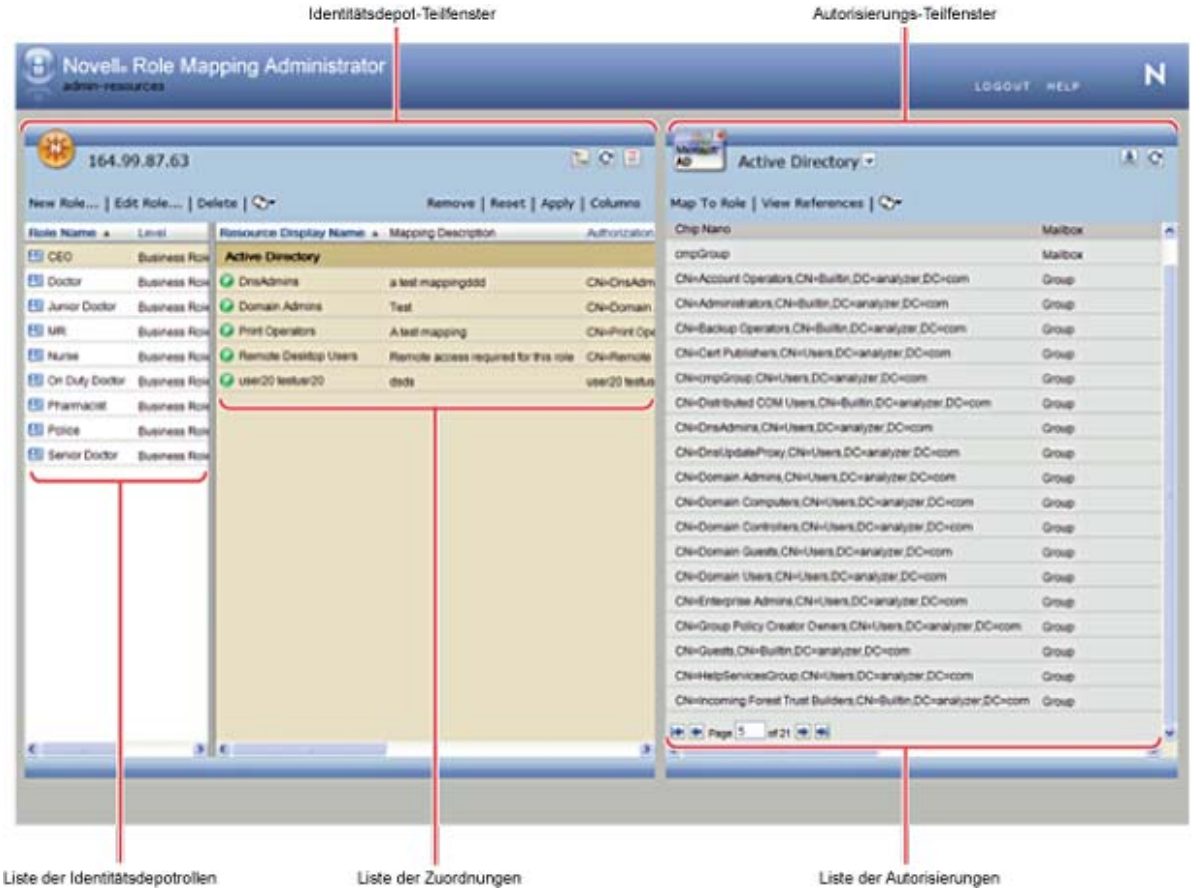
Abbildung 5-4 *Novell iManager*



5.4 Rollenzuordnungsadministrator

Der Rollenzuordnungsadministrator ist ein Webservice, der die Autorisierungen und Berechtigungen ermittelt, die innerhalb Ihres Haupt-IT-Systems erteilt werden können. Er ermöglicht es Geschäftsanalysten, nicht nur IT-Administratoren, bestimmte Autorisierungen für bestimmte Geschäftsrollen zu definieren und zu verwalten.

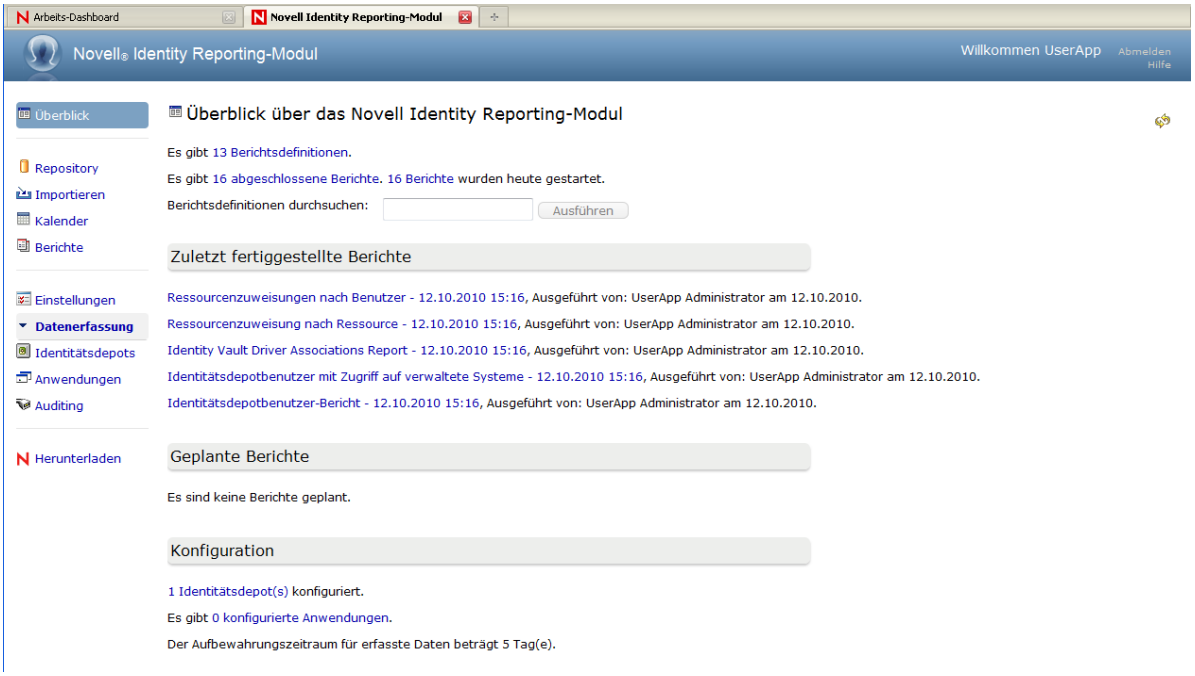
Abbildung 5-5 *Rollenzuordnungsadministrator*



5.5 Identitätsberichterstellung

Mit dem Identitätsberichterstellungsmodul können Sie Berichte generieren, die unternehmenskritische Informationen zu verschiedenen Aspekten Ihrer Identity Manager-Konfiguration liefern, einschließlich erfasster Informationen zu Identitätsdepots oder verwalteten Systemen, z. B. Active Directory oder SAP. Das Berichterstellungsmodul enthält eine Reihe von vordefinierten Berichtsdefinitionen, die Sie zum Generieren von Berichten verwenden können. Zusätzlich haben Sie die Möglichkeit, benutzerdefinierte Berichte zu importieren, die in einem Drittanbieter-Werkzeug definiert sind. Über die Benutzeroberfläche des Berichterstellungsmoduls können Sie problemlos festlegen, dass die Berichtgenerierung außerhalb der Hauptgeschäftszeit ausgeführt und somit die Systemleistung nicht beeinträchtigt wird.

Abbildung 5-6 *Identitätsberichterstellungsmodul*



Das Berichterstellungsmodul bietet mehrere offene Integrationspunkte. Wenn Sie beispielsweise Daten über Anwendungen von Drittanbietern erfassen möchten, die nicht mit Identity Manager verbunden sind, können Sie einen benutzerdefinierten REST-Endpunkt implementieren, um Daten von diesen Anwendungen zu erfassen. Darüber hinaus können Sie die Daten anpassen, die per Push-Verfahren in das Identitätsdepot übertragen werden. Wenn diese Daten verfügbar sind, können Sie benutzerdefinierte Berichte schreiben, um diese Informationen anzuzeigen.

6 Aktionen in Identity Manager

Identity Manager umfasst vier Komponenten:

- Die Identity Manager-Engine, die das Framework bereitstellt.
- Die Identity Manager-Richtlinien, die die Zuordnung von Attributen und Klassen sowie die Übereinstimmung und Erstellung von Einträgen steuern.
- Ereignisfilter, die die Richtung der Datensynchronisierung steuern.
- Das Identity Manager-Treiberschnittstellenmodul, das als Schnittstelle zwischen der Anwendung und der Identity Manager-Engine fungiert.

In diesem Abschnitt werden kurz die Identity Manager-Prozesse und -Aktionen erklärt. Die Identity Manager-Architektur wird hier nicht behandelt. Diese Informationen werden ansatzweise im Abschnitt Kapitel 4, „Identity Manager-Architektur“, auf Seite 29 erklärt. Eine detaillierte Erklärung zur Identity Manager-Architektur finden Sie in der Entwicklungsdokumentation.

Sie müssen die folgenden Abschnitte der Reihe nach lesen, um den Ereignisfluss und die Prozesse zu verstehen, die auf die Ereignisse in Identity Manager und das verbundene System angewendet werden.

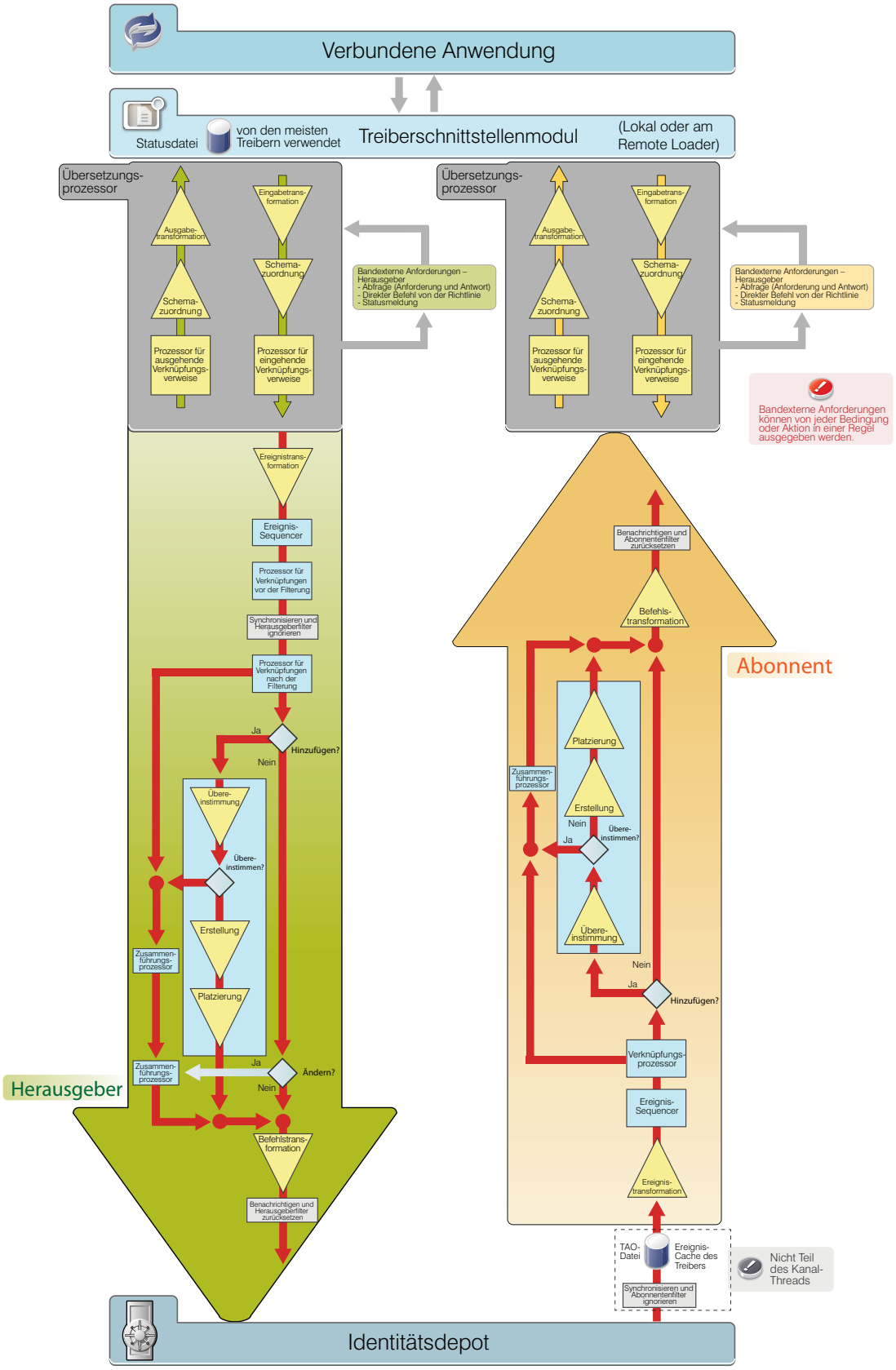
- Abschnitt 6.1, „Identitätsdepot“, auf Seite 50
- Abschnitt 6.2, „Schnittstellenmodul“, auf Seite 52
- Abschnitt 6.3, „Kanäle“, auf Seite 53
- Abschnitt 6.4, „Ereignisse und Befehle“, auf Seite 53
- Abschnitt 6.5, „Schemazuordnungsrichtlinie“, auf Seite 54
- Abschnitt 6.6, „Ereignistransformationsregel“, auf Seite 54
- Abschnitt 6.7, „Filter“, auf Seite 55
- Abschnitt 6.8, „Hinzufügeprozessor“, auf Seite 57
- Abschnitt 6.9, „Übereinstimmungsregel“, auf Seite 58
- Abschnitt 6.10, „Erstellungsregel“, auf Seite 59
- Abschnitt 6.11, „Platzierungsregel“, auf Seite 59
- Abschnitt 6.12, „Befehlstransformationsregel“, auf Seite 60
- Abschnitt 6.13, „Regeln, Richtlinien und Formatvorlagen“, auf Seite 61

6.1 Identitätsdepot

Das Identitätsdepot ist ein Repository von Identitätsinformationen. Es wird auch als Novell eDirectory-Baum bezeichnet. Im Identitätsdepot werden Identity Manager-spezifische Informationen gespeichert, z. B. Treiberkonfigurationen, Parameter und Richtlinien.

Das Identitätsdepot kann im engeren Sinn als privater Datenspeicher für Identity Manager gesehen werden, im weiteren Sinn als Metaverzeichnis mit Unternehmensdaten, die auf verschiedenen Anwendungen synchronisiert werden sollen, einschließlich verschiedenen Verzeichnissen, Datenbanken, Telefonsystemen, Betriebssystemen und HR-Systemen. Das Identitätsdepot verfügt über ein umfangreiches Schema, das angepasst werden kann. Die Daten im Depot stehen für alle Protokolle zur Verfügung, die von eDirectory unterstützt werden, einschließlich NCP (NetWare Core Protocol), LDAP und DSML. Identity Manager bietet keine zentrale Verwaltungsmöglichkeit und löst auch nicht das Problem mehrerer Administratoren mit einem eigenen Administrator für jede Anwendung. Das Programm löst allerdings das Problem doppelter, inkonsistenter Daten in den einzelnen Anwendungen. Beispielsweise werden Daten, die von einem PeopleSoft-System zu Lotus Notes synchronisiert wurden, zunächst dem Identitätsdepot hinzugefügt und dann an das Lotus Notes-System gesendet. In einer typischen Identitätsdepotumgebung befindet sich ein Identitätsdepot im Zentrum, an das andere Anwendungen angeschlossen sind. Die Identity Manager-Architektur kann man sich als mehrere Eins-zu-Eins-Beziehungen oder als Speichennetz vorstellen. Jede einzelne Beziehung besteht zwischen dem Identity Manager-Identitätsdepot und einer bestimmten verbundenen Anwendung.

Abbildung 6-1 *Fehlerbaumanalyse*



Ein Treiber ist ein Anwendungsschnittstellenmodul, das mit Richtlinien kombiniert ist und Identity Manager die Kommunikation mit einer externen Anwendung ermöglicht, um Daten zwischen der Anwendung und dem Identitätsdepot zu synchronisieren. Beachten Sie, dass die Begriffe „Treiber“ und „Schnittstellenmodul“ synonym sind. In Abbildung 6-1 befindet sich das Schnittstellenmodul oben, verknüpft mit einer externen Anwendung und dem Identitätsdepot. Zwischen dem Treiberschnittstellenmodul und dem Identitätsdepot bestehen Regeln, die die Daten verwalten.

Datenflüsse durch ein Identity Manager-System in Form von XML-Dokumenten In Identity Manager gibt es ein XML-Vokabular namens XDS, das zur Darstellung des Status von Objekten und Datenvorgängen mit den entsprechenden Attributwerten verwendet wird.

Die Identity Manager-Engine ruft über das Schnittstellenmodul Informationen von einem verbundenen System ab und stellt Informationen in ein verbundenes System ein. Anhand der Treiberkonfigurationsregeln entscheidet sie, was zu tun ist und wie.

Treiber stellen eine Verbindung zur Anwendung her, um Objekte und Entitäten zu verwalten. Ein Treiber ist hauptsächlich für zwei Aufgaben zuständig:

- Er meldet Datenänderungen (Ereignisse) in der Anwendung an die Identity Manager-Engine.
- Er führt die Datenänderungen (Befehle), die von der Identity Manager-Engine übermittelt wurden, in der Anwendung aus.

Die Kombination aus dem Treiber des verbundenen Systems, den Anwendungsverbindungsinformationen und einem Satz von Richtlinien wird als Treiberkonfiguration bezeichnet. Treiberkonfigurationen werden in einem Satz von Verzeichnisobjekten im Identitätsdepot gespeichert. Das DirXML-Treiberobjekt enthält andere Objekte, die die Richtlinien und Parameter definieren, die mit der Konfiguration verknüpft sind.

Die Treiberkonfiguration definiert eine Daten-Pipeline zwischen einer Anwendung und dem Identitätsdepot. Die Treiberkonfiguration definiert, was synchronisiert werden kann und wie das eDirectory-Schema einem verbundenen Anwendungsschema oder Metadaten zugeordnet werden soll. Beispielsweise könnte der Vorname eines Benutzers in einer HR-Anwendung als „Rufname“ bezeichnet werden, im Identitätsdepot dagegen als „Vorname“. Im Namespace der Anwendung nennen Sie ihn „Rufname“, im Namespace des Identitätsdepots dagegen „Vorname“. In Identity Manager arbeiten Sie normalerweise mit den Attributnamen in der Namespace des Identitätsdepots.

Zwischen einem Identitätsdepotobjekt und einem Anwendungsobjekt wird eine Beziehung aufgebaut, wenn die beiden Objekte dieselbe Entität darstellen. Diese Beziehung wird als Verknüpfung bezeichnet und im Identitätsdepot im verknüpften Identitätsdepotobjekt gespeichert. Die Verknüpfung baut eine Beziehung zwischen dem Identitätsdepotobjekt und dem Objekt im verknüpften System auf. Schlüsselwerte, die einmalig Objekte in verbundenen Systemen erkennen: Globale eindeutige Bezeichner (GUIDs), DNs, Primärschlüssel in Datenbanken etc. Jeder Treiber ist kodiert und verwendet einen spezifischen Schlüssel.

6.2 Schnittstellenmodul

Ein Schnittstellenmodul ist ein kompilierter Code, der die Befehle und Daten zwischen einer Anwendung und Identity Manager überträgt. Das Treiberschnittstellenmodul ist oft in Java geschrieben, das native Aufrufe der Anwendungsprogrammierschnittstelle (Application Programming Interface, API) verwendet, die das System den Entwicklern zur Verfügung stellt.

Hierbei kann es sich um LDAP-Standardaufrufe, native Windows Active Directory-Aufrufe oder auch JDBC-Verbindungen für SQL-Datenbanken handeln. Das Schnittstellenmodul ist für folgende Aufgaben zuständig:

- Übersetzen der Informationen in der Anwendung in ein Standard-XML-Dokument
- Herstellen und Warten der Verbindung zur verbundenen Anwendung
- Verwalten der von Identity Manager und der verbundenen Anwendung gesendeten Befehle
- Überwachen der verbundenen Anwendung auf Änderungen

Wenn beispielsweise das verbundene System ein HR-System ist und ein neuer Mitarbeiter eingestellt wird, muss das Schnittstellenmodul ein XML-Dokument erstellen, das diese Informationen beschreibt. In Identity Manager-Terminologie ist dies ein Ereignis vom Typ „Hinzufügen“, und ein XML-Dokument wird erstellt, um dieses Ereignis der Engine zu erklären. Das Ereignis wird an die Engine gesendet und ein neuer Benutzer wird am angegebenen Standort erstellt. Nachdem das neue Benutzerobjekt im Identitätsdepot erstellt wurde, wird ein Ereignis für andere Treiber erstellt, die Änderungen an Benutzerobjekten überwachen. Wenn Sie beispielsweise den GroupWise-Treiber bereitgestellt haben, wird ein Ereignis vom Typ „Hinzufügen“ für den GroupWise-Treiber erstellt, um ein Email-Postfach für den neuen Benutzer zu erstellen.

6.3 Kanäle

Der Datenfluss zwischen dem Identitätsdepot und einem verbundenen System verläuft in zwei Richtungen, die Herausgeber und Abonnent genannt werden. Diese Richtungen werden aus Sicht der Anwendung benannt:

- Der Abonnentenkanal ist der Kanal, in dem Daten vom Identitätsdepot über das Schnittstellenmodul an die Anwendung fließen. Die Anwendungen abonnieren die Daten vom Identitätsdepot.
- Der Herausgeberkanal ist der Kanal, in dem die Daten von der Anwendung zum Identitätsdepot fließen. Die Anwendungen veröffentlichen Daten im Identitätsdepot.

In einigen Fällen kann die Richtlinie verursachen, dass Daten in einem Kanal rückwärts fließen. Dies wird als Zurückschreiben im Kanal bezeichnet.

6.4 Ereignisse und Befehle

Der Unterschied zwischen Ereignissen und Befehlen ist zwar gering, doch wichtig. Die Meldung einer Änderung an Daten bei einer Eingabe in den Kanal ist ein Ereignis. Ereignisse treten sowohl im Identitätsdepot als auch im verbundenen System auf. Beispiele von Ereignissen:

- Erstellung eines Objekts
- Änderung von Objektattributwerten
- Änderung eines Objektnamens
- Verschiebung eines Objekts in der Objekthierarchie
- Löschung eines Objekts

Befehle sind die Ausgabe eines Treiberkanals. Wenn das Schnittstellenmodul eine Ereignisbenachrichtigung an Identity Manager sendet, informiert es Identity Manager über eine Änderung an den Daten, die in der Anwendung vorgenommen wurde. Identity Manager legt dann basierend auf den konfigurierbaren Befehlen fest, welche Befehle gegebenenfalls an das

Identitätsdepot gesendet werden müssen. Wenn Identity Manager einen Befehl an das Schnittstellenmodul sendet, hat Identity Manager bereits ein Identitätsdepot-Ereignis als Eingabe verarbeitet, die entsprechenden Richtlinien angewendet und festgelegt, dass die durch den Befehl dargestellte Änderung in der Anwendung erforderlich ist.

Ein Ereignis aus dem Identitätsdepot wird über den Abonnentenkanal gesendet und schließlich in einen Befehl umgewandelt, der an das Treiberschnittstellenmodul übermittelt wird, wo es einige Änderungen im verbundenen System verursachen soll. Ein Ereignis aus der Anwendung wird über den Herausgeberkanal gesendet und schließlich in einen Befehl umgewandelt, der an das Identitätsdepot übermittelt wird, wo es die in der Anwendung vorgenommene Änderung synchronisieren soll. Wenn aus Sicht des Gesamtsystems ein Befehl von einem Treiber in dessen Herausgeberkanal ein Objekt im Identitätsdepot erstellt oder aktualisiert, könnte dies verursachen, dass Ereignisse an die Abonnentenkanäle anderer Treiber im System übertragen werden. Dadurch können Änderungen kaskadiert werden und an alle verbundenen Systeme fließen.

6.5 Schemazuordnungsrichtlinie

Die Schemazuordnungsrichtlinie betrifft sowohl den Abonnentenkanal als auch den Herausgeberkanal. Der Zweck der Schemazuordnungsrichtlinie besteht darin, Schemanamen (insbesondere Attributnamen und Klassennamen) zwischen der Namespace des Identitätsdepots und der Namespace der Anwendung zuzuordnen. Die Schemazuordnungsrichtlinie wird vor der Ausgabetransformationsrichtlinie angewendet, wenn Identity Manager ein Dokument an das Schnittstellenmodul überträgt oder zurücksendet, und nach der Eingabetransformationsrichtlinie, wenn der Treiber ein Dokument an Identity Manager überträgt oder zurücksendet. Beispielsweise verwendet das HR-System „Rufname“ und das Identitätsdepot „Vorname“, wenn sich beide auf dasselbe Attribut beziehen. Die Schemazuordnungsrichtlinie verarbeitet die Änderung in Namen zwischen der Namespace der Anwendung und der Namespace des Identitätsdepots. Die Schemazuordnungsrichtlinie ist bidirektional. Sie überlappt beide Kanäle. Im Herausgeberkanal werden die Anwendungsnamen dem Identitätsdepot zugeordnet. Im Abonnentenkanal werden die Identitätsdepotnamen der Anwendung zugeordnet.

6.6 Ereignistransformationsregel

Die Ereignistransformationsregel wird auf Ereignisse angewendet, die bei einer Kanaleingabe gemeldet werden. Der Abonnentenkanal und der Herausgeberkanal haben normalerweise verschiedene Ereignistransformationsregeln. Der Zweck der Ereignistransformationsregeln besteht darin, die Meldung der Ereignisse zu ändern, bevor die Ereignisse von Identity Manager weiterverarbeitet werden.

Für die Ereignistransformationsregel gibt es viele allgemeine Anwendungen:

- Bereichsfilterung (wenn beispielsweise nur Ereignisse an Objekten in einem bestimmten Unterbaum oder mit einem bestimmten Attributwert zugelassen werden sollen)
- Benutzerdefinierte Ereignisfilterung (wenn beispielsweise keine Verschiebungen oder Löschungen zugelassen werden sollen)
- Übertragung des Ereignisses direkt in einen benutzerdefinierten Befehl zur Weiterleitung an das verbundene System
- Erstellen zusätzlicher Ereignisse

- Abschnitt 6.6.1, „Herausgeber“, auf Seite 55
- Abschnitt 6.6.2, „Abonnent“, auf Seite 55

6.6.1 Herausgeber

Die Eingabe an den Herausgeberkanal ist eine Beschreibung eines Ereignisses, das vom verbundenen System kommt. Der Zweck der Ereignistransformationsregel besteht darin, diese Beschreibung des vom Schnittstellenmodul an Identity Manager ausgegebenen Ereignisses zu ändern. Sie wird nach der Eingabetransformationsrichtlinie und Schemazuordnungsrichtlinie angewendet, aber vor jeder anderen richtlinienbasierten Ereignisverarbeitung. Die in der Ereignistransformationsregel implementierten Richtlinien werden für das Ereignis ausgeführt, wie zum Beispiel Ereignisse vom Typ „Hinzufügen“, „Löschen“ oder „Ändern“, nicht aber für die Daten. Sie können beispielsweise eine Richtlinie erstellen, die verhindert, dass der Administrator des verbundenen Systems neue Objekte im Identitätsdepot erstellt, oder Sie können Ereignisse vom Typ „Löschen“ verarbeiten, sodass ein Objekt, das im verbundenen System gelöscht wird, tatsächlich nur dazu führen könnte, dass das verknüpfte Identitätsdepotobjekt geändert wird.

Wenn ein Vorgang vom Typ „Hinzufügen“ in einen Vorgang vom Typ „Zusammenführen“ konvertiert wird, wird das aktuelle Dokument wie der Vorgang vom Typ „Künstliches Hinzufügen“ verworfen und der Filter wird dazu verwendet, alle Werte sowohl vom verbundenen System als auch vom Identitätsdepot abzufragen. Die Einstellung für jedes Attribut im Filter wird verwendet, um zu entscheiden, was mit den Daten geschehen soll. Optional können die Quellinformationen mit den Informationen vom Ziel überschrieben, das Ziel mit der Quelle überschrieben, beide Methoden kombiniert und beide mit den Ergebnissen aktualisiert werden oder es kann einfach nichts getan werden.

Wenn ein Ereignis vom Typ „Hinzufügen“ einen Verknüpfungswert enthält, wandelt die Identity Manager-Engine dieses Ereignis in ein Ereignis vom Typ „Ändern“ um.

6.6.2 Abonnent

Die Eingabe an den Abonnentenkanal ist eine Beschreibung eines Ereignisses, das vom Identitätsdepot kommt. In vielen Fällen könnte der Filter dazu verwendet werden, die gewünschten Objekttypen sowie die Attribute dieser Objekte festzulegen, doch die Ereignistransformationsrichtlinie kann dazu verwendet werden, die Ereignisse weiter anzupassen. Dies wird manchmal als Bereichsfilterung bezeichnet und ermöglicht eine viel feinere Steuerung der Daten. Sie können beispielsweise Filter zur Angabe von Benutzerobjekten verwenden. Er nimmt an, dass Sie alle Benutzer synchronisieren möchten. Wenn ein verbundenes System auf eine Teilmenge aller Benutzer beschränkt ist, dann wird die Ereignistransformation verwendet, um zu entscheiden, ob ein Ereignis für ein Objekt im Bereich liegt oder nicht. Wenn beispielsweise in Ihrem verbundenen System nur Benutzer mit einem Abteilungsattribut „Vertrieb“ vorhanden sein sollen, dann können Sie eine Regel in der Ereignistransformationsrichtlinie erstellen, die alle Ereignisse für Benutzer blockiert, die nicht das Abteilungsattribut „Vertrieb“ enthalten.

6.7 Filter

Der Filter steuert den Datenfluss zwischen dem Identitätsdepot und dem verbundenen System. Der Filter spielt in einer Identity Manager-Treiberkonfiguration verschiedene Rollen. Abbildung 6-1 zeigt den Filter an vier Stellen, die die meisten seiner Rollen darstellen, doch es gibt eigentlich nur einen Filter für den Treiber.

Während die Kanäle den Datenfluss zulassen, werden Richtlinien und Filter in den Kanälen platziert, um zu regulieren, was durchkommt und wie es bei Ankunft am Ziel aussieht. Beispielsweise können Sie durch Konfigurieren des Treiberfilters einen Attributwert blockieren, sodass zum Beispiel eine Telefonnummer vom verbundenen System nicht im Identitätsdepot ankommt und umgekehrt.

Dadurch kann gesteuert werden, ob das Identitätsdepot oder das verbundene System die autorisierte Quelle zum Erfüllen bestimmter Geschäftsanforderungen ist. Wenn beispielsweise der Filter für die Beziehung zwischen dem PBX-System und dem Identitätsdepot es zulässt, dass die Telefonnummer eines Mitarbeiters vom PBX-System in das Identitätsdepot, jedoch nicht vom Identitätsdepot zum PBX-System fließt, ist das PBX-System die autorisierte Quelle für die Telefonnummer. Wenn alle anderen Beziehungen verbundener Systeme zulassen, dass die Telefonnummer vom Identitätsdepot zu den verbundenen Systemen fließt, jedoch nicht in die umgekehrte Richtung, bedeutet dies, dass das PBX-System die einzige autorisierte Quelle für Telefonnummern von Mitarbeitern im Unternehmen ist.

Der Treiberfilter gibt die Klassen der Objekte und die Attribute dieser Objekte an, für die das Identitätsdepot Ereignisse und Befehle für beide Kanäle verarbeitet. Er gibt der Metaverzeichnis-Engine Anweisungen zu Ereignissen und Informationen, die für die Konfiguration des Treibers von Interesse sind. Auf seiten des Identitätsdepots werden Ereignisse für den Treiber in die Warteschlange gestellt, wenn sie mit einer Objektklasse im Filter übereinstimmen und wenn sie mit einem Attribut übereinstimmen, das auf „Synchronisieren“, „Benachrichtigen“ oder „Zurücksetzen“ festgelegt wurde. Ereignisse, die im Identitätsdepot auftreten und nicht mit den im Filter angegebenen Datentypen übereinstimmen, werden von diesem Treiber ignoriert. Bei der Anwendung ist es ähnlich, d. h., aufgetretene Ereignisse, die nicht mit den im Filter angegebenen Filtertypen übereinstimmen, werden ignoriert. Allerdings muss das Schnittstellenmodul diese Ereignisse möglicherweise doch noch überprüfen, um festzustellen, ob sie verarbeitet werden müssen. Wenn beispielsweise der Identity Manager-Treiber nur Benutzerinformationen synchronisieren sollte, gibt der Filter Benutzerobjekte an und die Änderung in andere Identitätsdepotobjekte wird ignoriert. Von den möglichen Benutzerklassenattributen gibt der Filter die ausgewählten Attribute an, wie zum Beispiel CN, Vorname, Nachname und Telefonnummer. Änderungen in andere Benutzerklassenattribute werden ignoriert. Die Benutzerobjektklasse und der Satz der entsprechenden Datenattribute werden für die meisten verbundenen Systeme im Filter aufgeführt.

- Abschnitt 6.7.1, „Synchronisierungsattribut“, auf Seite 56
- Abschnitt 6.7.2, „Benachrichtigungsattribut“, auf Seite 56

6.7.1 Synchronisierungsattribut

Wenn im Herausgeberkanal ein Ereignis einmal für die Verarbeitung im Kanal in die Warteschlange gestellt wurde und die Eingabetransformation, die Schemazuordnung und die Ereignistransformation durchlaufen hat, dann werden die Synchronisierungsattribute aus dem Eingabedokument ausgewählt und alle Attribute, die nicht auf „Synchronisieren“ oder „Benachrichtigen“ festgelegt wurden, werden entfernt. Attribute, die auf „Zurücksetzen“ festgelegt wurden, werden auch durch Abfragen des Identitätsdepots nach dem korrekten Wert verarbeitet. Der korrekte Wert wird an die Anwendung zurückgesendet, um die gerade vorgenommene Änderung rückgängig zu machen. Im Abonnentenkanal arbeitet der Synchronisierungsfilter genauso wie für den Herausgeberkanal. Der einzige Unterschied besteht darin, dass Ereignisse vom Identitätsdepot anstatt vom verbundenen System kommen.

6.7.2 Benachrichtigungsattribut

Mit dem Benachrichtigungsattribut können Sie Attributdaten vom Ereignisdokument verwenden, ohne die Daten mit dem Identitätsdepot synchronisieren zu müssen. Sie benötigen beispielsweise den Vornamen, zweiten Vornamen und Familiennamen einer Person aus dem HR-System, um ein Konto zu erstellen, möchten aber den zweiten Vornamen nicht im Identitätsdepot speichern. Wenn Sie das Attribut des zweiten Vornamens auf „Benachrichtigen“ festlegen, können Sie auf den

Attributwert zugreifen, ohne ihn im Identitätsdepot speichern zu müssen. Alle auf „Benachrichtigen“ festgelegten Attribute werden vor der Übermittlung an das Ziel aus dem Dokument entfernt.

6.8 Hinzufügeprozessor

- Abschnitt 6.8.1, „Herausgeber“, auf Seite 57
- Abschnitt 6.8.2, „Abonnent“, auf Seite 57

6.8.1 Herausgeber

Der Hinzufügeprozessor wird verwendet, um zu entscheiden, ob es sich um ein Dokument vom Typ „Hinzufügen“ handelt. Dies ist eine Verzweigung in der Verarbeitung des Ereignisses im Treiber. Wenn es sich um ein Ereignis vom Typ „Hinzufügen“ handelt, wird es von der Übereinstimmungsregel verarbeitet. Das Schnittstellenmodul stellt den Verknüpfungswert bereit und ermöglicht es der Identity Manager-Engine somit, das korrekte Objekt schnell und leicht im Identitätsdepot aufzufinden. Verknüpfungen werden als Übereinstimmung zwischen zwei Objekten erstellt oder wenn ein Objekt entweder im Identitätsdepot oder im verbundenen System neu erstellt wird. Nachdem eine Verknüpfung zwischen Objekten hergestellt wurde, bleibt diese gültig, bis die Objekte gelöscht werden oder bis die Verknüpfung vom Administrator gelöscht wird. Sorgfältig entwickelte Übereinstimmungsregeln automatisieren die Erstellung von Verknüpfungen zwischen vorhandenen Objekten im Identitätsdepot und dem verbundenen System. Weitere Informationen finden Sie unter Abschnitt 6.13.3, „Verknüpfungen“, auf Seite 64.

Wenn es sich nicht um ein Ereignis vom Typ „Hinzufügen“ handelt, wird es im nächsten Schritt an die Befehlstransformation weitergeleitet.

6.8.2 Abonnent

Im Abonnentenkanal wird der Hinzufügeprozessor verwendet, um zu entscheiden, ob es sich bei einem Ereignis um ein Ereignis vom Typ „Hinzufügen“ handelt. Wenn es sich um ein Ereignis vom Typ „Hinzufügen“ handelt, wird es von der Übereinstimmungsregel verarbeitet. Die Identity Manager-Engine verwendet den Verknüpfungswert eines Identitätsdepotobjekts, um dem Schnittstellenmodul die Änderung des korrekten Objekts im verbundenen System zu ermöglichen. Weitere Informationen finden Sie unter Abschnitt 6.13.3, „Verknüpfungen“, auf Seite 64.

Wenn es sich nicht um ein Ereignis vom Typ „Hinzufügen“ handelt, wird es im nächsten Schritt an die Befehlstransformation weitergeleitet.

Wenn ein Ereignis vom Typ „Ändern“ keine Verknüpfung enthält, die ein tatsächliches Objekt bei Ankunft im Hinzufügeprozessor auflöst, versucht die Identity Manager-Engine es zu erstellen. Dies ist der Vorgang des künstlichen Hinzufügens, der sowohl im Herausgeber- als auch im Abonnentenkanal ausgeführt werden kann.

Die Identity Manager-Engine verwendet das Ereignis vom Typ „Ändern“, um herauszufinden, mit welchem Objekt gearbeitet werden soll. Sie verwendet dann den Filter für Rückfragen, um alle Attribute abzurufen, die für dieses Objekt verfügbar und im aktuellen Kanal auf „Synchronisieren“ oder „Benachrichtigen“ festgelegt sind. Sie verwirft das Ereignis vom Typ „Ändern“ und erstellt ein Ereignis vom Typ „Hinzufügen“, das es ersetzt. Das Ereignis vom Typ „Hinzufügen“ wird durch die Übereinstimmungs-, Erstellungs-, Platzierungs- und Befehlstransformation geleitet (im Abonnenten

durchläuft es außerdem noch die Schemazuordnung und Ausgabetransformation). Die Ereignistransformationsregel wird nicht auf Vorgänge des künstlichen Hinzufügens angewendet. Der Grund dafür ist der Standort der Regel vor dem Hinzufügeprozessor.

6.9 Übereinstimmungsregel

Übereinstimmungsregeln erstellen Links zwischen einem vorhandenen Objekt im Identitätsdepot und einem vorhandenen Objekt im verbundenen System. Die Übereinstimmungsregeln geben an, welche Klassen- und Attributwerte für ein Objekt im Identitätsdepot und ein Objekt im verbundenen System übereinstimmen müssen, um als entsprechende Einträge gekennzeichnet zu werden.

Eine gute Übereinstimmungsregel veranlasst Sie, beide betroffenen Systeme zu untersuchen und die Daten zu finden, die eine 1:1-Übereinstimmung zwischen beiden garantiert. Attribute wie die ID-Nummer des Mitarbeiters, die Email-Adresse und Ausweisnummer sind einige der üblichen Daten, die als Übereinstimmungskriterien verwendet werden. Wenn kein Attribut verfügbar ist, kann eine Kombination von Attributen verwendet werden. Ein Übereinstimmung des Nachnamens ist kein gutes Kriterium. In größeren Unternehmen ist es beispielsweise möglich, dass zwei Mitarbeiter denselben Nachnamen haben. Eine Übereinstimmung von Nachname + Vorname würde die Qualität der Übereinstimmung schon verbessern, eine Übereinstimmung von Nachname + Vorname + Abteilung würde die Wahrscheinlichkeit einer korrekten Übereinstimmung noch weiter erhöhen. Wenn eine Übereinstimmung erfolgreich ist, wird eine Verknüpfung zwischen den beiden Objekten erstellt. Wenn eine Übereinstimmung nicht erfolgreich ist, werden die Erstellungsregeln angewendet.

- Abschnitt 6.9.1, „Herausgeber“, auf Seite 58
- Abschnitt 6.9.2, „Abonnent“, auf Seite 58

6.9.1 Herausgeber

Die Übereinstimmungsregel wird verwendet, um ein Objekt im Identitätsdepot mit dem entsprechenden Objekt in der Anwendung zu verknüpfen. Die Übereinstimmungsregel verwendet Übereinstimmungskriterien und fragt im Identitätsdepot nach, ob ein übereinstimmendes Objekt vorhanden ist. Die Übereinstimmungsregel gibt Null zurück, wenn kein Objekt übereinstimmt, sodass das Ereignis vom Typ „Hinzufügen“ weiter verarbeitet wird. Sie gibt Eins zurück, wenn ein übereinstimmendes Objekt gefunden wurde, was bedeutet, dass das Objekt im Eingabedokument mit einem Objekt im Identitätsdepot übereinstimmt. Wenn die Objekte übereinstimmen, werden die Daten der beiden Objekte basierend auf den Filtereinstellungen zusammengeführt. Wenn die Übereinstimmungsregel mehr als ein übereinstimmendes Objekt findet, behandelt die Identity Manager-Engine dies als einen Fehler und beendet die Transaktion. Sie sollten die Übereinstimmungsregel entweder ändern oder diesen Konflikt manuell beheben.

6.9.2 Abonnent

Im Abonnentenkanal wird die Übereinstimmungsregel auf die Ereignisse vom Typ „Hinzufügen“ angewendet. Sie verwendet die Identitätsdepotdaten, um das verbundene System nach übereinstimmenden Objekten abzufragen. Die Fähigkeit zum Abfragen des verbundenen Systems über das Schnittstellenmodul hängt von der Schemazuordnung ab, um die Änderungen an der Formatierung der Namen in der Anwendung rückgängig zu machen. Sie kann aber auch von der Ausgabetransformation abhängen.

6.10 Erstellungsregel

Die Erstellungsregeln werden auf die Ereignisse vom Typ „Hinzufügen“ angewendet, wenn die Übereinstimmungsregeln keine Übereinstimmung finden. Die Erstellungsregeln geben die minimale Anzahl der Daten an, die ein Ereignis aufweisen muss, bevor ein Objekt im Identitätsdepot oder im verbundenen System erstellt werden kann.

- Abschnitt 6.10.1, „Herausgeber“, auf Seite 59
- Abschnitt 6.10.2, „Abonnent“, auf Seite 59

6.10.1 Herausgeber

Wenn die Übereinstimmungsregel kein übereinstimmendes Objekt im Identitätsdepot findet, wird auf das Dokument die Erstellungsregel angewendet, um sicherzustellen, dass das Dokument genügend Informationen enthält. Sie wird auch verwendet, um Standardwerte für Attribute anzugeben, und könnte eine Vorlage zur Erstellung eines neuen Objekts angeben. Für Objekte, die im Identitätsdepot synchronisiert werden, kann es obligatorische Attribute im Schema geben, die zur Erstellung eines Benutzers erforderlich sind, wie zum Beispiel CN und Nachname. Verschiedene Objektklassen und Anwendungsfälle können verschiedene Anforderungen haben.

Die Erstellungsregel kann auch ein Ereignis vom Typ „Hinzufügen“ verhindern, wenn dieses Ereignis nicht den von der Erstellungsregel festgelegten Bedingungen entspricht. Wenn beispielsweise die Erstellungsregel besagt, dass ein Objekt eine Telefonnummer aufweisen muss, dann schlägt das Ereignis vom Typ „Hinzufügen“ fehl, falls keine Telefonnummer angegeben ist.

Die verworfenen Ereignisse werden erneut verarbeitet, sobald die zusätzlichen Attributinformationen im verbundenen System hinzugefügt werden. Dies führt zu einem Ereignis vom Typ „Ändern“ ohne ein verknüpftes Objekt, das der Hinzufügeprozessor in einen Vorgang des künstlichen Hinzufügens konvertiert.

6.10.2 Abonnent

Die Erstellungsregel im Abonnenten funktioniert genauso wie im Herausgeberkanal, wenn festgelegt wird, ob ein Ereignis genügend Informationen zur Erstellung eines Objekts im verbundenen System aufweist. Dazu sind Kenntnisse über das verbundene System und dessen technische oder geschäftliche Anforderungen erforderlich.

Die Erstellungsregel wird oft verwendet, um die für das neue Objekt verfügbaren Attribute (aus dem ursprünglichen Ereignis) zu prüfen und verhindert die Erstellung des neuen Objekts, falls ein oder mehrere Attribute fehlen. Das häufigste Beispiel dazu im Abonnentenkanal ist die Passwortanforderung. Normalerweise wird ein Benutzer im Identitätsdepot in zwei Stufen erstellt, zunächst als Benutzerobjekt, woraufhin in einem zweiten Vorgang ein Passwort festgelegt wird. Es kommt häufig vor, dass ein Objekt erstellt wird, doch die Erstellungsregel fehlschlägt, weil das Passwort fehlt, das ein erforderliches Attribut zur Erstellung eines neuen Benutzerobjekts ist. Wenn dann das Passwortereignis kurz darauf durchgeführt wird, kann das neue Objekt erfolgreich hinzugefügt werden.

6.11 Platzierungsregel

- Abschnitt 6.11.1, „Herausgeber“, auf Seite 60
- Abschnitt 6.11.2, „Abonnent“, auf Seite 60

6.11.1 Herausgeber

Wenn die Übereinstimmungsregel keine übereinstimmenden Objekte findet und die Erstellungsregel bestätigt, dass das Ereignis die Mindestanforderungen erfüllt, gibt die Platzierungsregel an, welches Objekt erstellt und wo es platziert wird. Für den Herausgeberkanal wird das Objekt im Identitätsdepot platziert und es hat einen eindeutigen Namen (oder eine eindeutige ID), um es zu benennen, und einen Container, in den es gestellt wird. Da die Platzierungsregeln den Standort festlegen, bestimmen sie auch den eindeutigen Namen der Objekte. Beispielsweise platziert das Identitätsdepot alle Objekte in den Container `Daten\Benutzer\jdoe`.

6.11.2 Abonnent

Im Abonnentenkanal funktioniert die Platzierungsregel genauso wie im Herausgeberkanal. Platzierungen in verbundenen Systemen können einfach oder komplex sein. Eine einfache Platzierungsregel platziert alle Objekte am selben Standort.

Für Platzierungen im verbundenen System sind detaillierte Kenntnisse darüber erforderlich, wie das verbundene System funktioniert. Ein einfaches Beispiel für eine Platzierung, nämlich Lotus Notes in der Standardkonfiguration, platziert alle Objekte im Container `CN=jdoe/O=novell`.

Ein komplexeres Beispiel könnte ein HR-Standortcode-Attribut verwenden, um festzulegen, wo ein Objekt platziert wird. Sie können eine Zuordnungstabelle verwenden, um leichter eine Beziehung zwischen einem Standort zur Platzierung und einem Attributwert aufbauen zu können.

6.12 Befehlstransformationsregel

Die Befehlstransformationsregel wird auf Befehle angewendet, die auf eine Kanalausgabe ausgegeben werden sollen. Der Abonnentenkanal und der Herausgeberkanal haben normalerweise verschiedene Ereignistransformationsregeln. Der Zweck der Befehlstransformationsregel besteht darin, die endgültige Verarbeitung von Befehlen vorzunehmen, bevor die Befehle an das Identitätsdepot oder das verbundene System gesendet werden.

Einige mögliche Anwendungen für die Befehlstransformationsregel:

- Ändern des Befehlstyps (ein Befehl zum Löschen eines Objekts kann beispielsweise in eine Änderung transformiert werden, die dazu führt, dass das Objekt archiviert wird)
- Blockieren von Befehlen
- Hinzufügen von weiteren Befehlen
- Steuern der Ausgabe des Vorgangs der Zusammanführung durch die Identity Manager-Engine

- Abschnitt 6.12.1, „Herausgeber“, auf Seite 60
- Abschnitt 6.12.2, „Abonnent“, auf Seite 61

6.12.1 Herausgeber

Hier wird die frühere Verzweigung am Hinzufügeprozessor wieder in den Fluss eingefügt. Alle Ereignisse werden von der Befehlstransformationsregel verarbeitet. Die meisten Treiberrichtlinien befinden sich in der Befehlstransformation, weil genau dort die Konversion vom Ereignis zum Befehl stattfindet. Bis zu diesem Punkt hat das Dokument ein Ereignis beschrieben, das im verbundenen

System aufgetreten ist. Nun wird dieses Ereignis in einen Befehl transformiert und auf das Identitätsdepot angewendet. Es ist die letzte Möglichkeit zur Änderung des Befehls, bevor er auf das Identitätsdepot angewendet wird.

6.12.2 Abonnent

Im Abonnentenkanal befinden sich die meisten Treiberrichtlinien in der Befehlstransformation, weil dies logischerweise der Vorgang ist, in dem die Konversion vom Ereignis zum Befehl stattfindet, bevor die Schemazuordnungsrichtlinie angewendet wird. Sowohl die Schemazuordnungsrichtlinie als auch die Ausgabetransformationsrichtlinie werden nach der Befehlstransformationsrichtlinie im Abonnentenkanal ausgeführt. Bis zu diesem Punkt hat das Dokument ein Ereignis beschrieben, das im Identitätsdepot aufgetreten ist. Nun wird dieses Ereignis in einen Befehl transformiert und auf das verbundene System angewendet.

6.13 Regeln, Richtlinien und Formatvorlagen

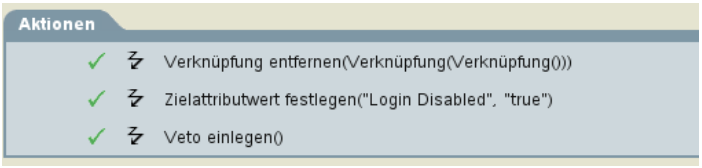
In Identity Manager ist eine Regel eine Sammlung von Richtlinien. Jede Regel hat Bedingungen, die eingehalten werden müssen, sowie Aktionen, die ausgeführt werden müssen, wenn die Bedingungen zutreffen. Die Grammatik der Bedingungen sollte für Menschen gut lesbar sein und Sinn machen. Beispielsweise wäre eine Bedingung „Wenn Objektklasse gleich Benutzer“ wahr, wenn das im aktuellen Dokument beschriebene Objekt ein Benutzerobjekt ist, und falsch, wenn das Objekt eine Gruppe ist. Bedingungen setzen sich aus Bedingungsgruppen zusammen. Innerhalb einer Bedingungsgruppe können alle Bedingungen mit UND bzw. ODER kombiniert werden, und das Ergebnis muss für die Bedingungsgruppe wahr sein, um als wahr evaluiert zu werden, andernfalls wird es als falsch evaluiert. Mehrere Bedingungsgruppen können ebenfalls mit UND und ODER kombiniert werden. Wenn die Bedingungsgruppe(n) als „Wahr“ evaluiert wurde(n), dann werden die Aktionen der Regel ausgeführt.

Abbildung 6-2 *Bedingungen für den Richtlinien-Builder*

Aktionen können für das aktuelle Dokument ausgeführt werden und in vielen Fällen reicht dies auch aus. Doch Aktionen können auch die Quelle oder das Ziel abfragen, also entweder das Identitätsdepot oder das verbundene System, abhängig davon, welchen Kanal Sie verwenden), um zusätzliche Informationen zu erhalten. Aktionen können das aktuelle Dokument ändern, um eine geänderte Version dieses Dokuments zu erstellen. Sie können das aktuelle Dokument aber auch vollständig sperren. Aktionen können verwendet werden, um unterschiedliche Dokumente zu erstellen. Ein Dokument, das ein Löschereignis in einem verbundenen System beschreibt, könnte von einer Bedingung getestet werden (wenn Aktion gleich Löschung). Es könnte einen Satz von Aktionen auslösen, um zu verhindern, dass das verknüpfte Objekt in eDirectory gelöscht wird (Veto) und

stattdessen dieses Objekt geändert wird, um dessen Verknüpfungswert für diese Anwendung zu entfernen (Verknüpfung-entfernen) und um es zu deaktivieren (Zielattributwert „Anmeldung deaktiviert“ auf „Wahr“ festlegen).

Abbildung 6-3 *Aktionen des Richtlinien-Builders*



Richtlinien definieren, welche Daten übertragen und wie die Daten zwischen dem verbundenen System und dem Identitätsdepot synchronisiert werden. Ein Standard-Richtliniensatz ist in der Treiberkonfiguration verfügbar. Andere Richtlinien sind möglicherweise lokale Anpassungen des Treibers. Sie können Richtlinien mit dem DirXML-Skript, XSLT oder dem ECMA-Skript schreiben.

Der Zweck einer Richtlinie besteht darin, Änderungen am Eingabedokument vorzunehmen und ein Ausgabedokument zu erzeugen. Die meisten Richtlinien werden entweder im Abonnentenkanal evaluiert oder im Herausgeberkanal. Die Schemazuordnungsrichtlinie, die Eingabetransformationsrichtlinie und die Ausgabetransformationsrichtlinie werden in beiden Kanälen evaluiert. Beispielsweise verwendet ein Unternehmen `inetOrgPerson` als Hauptbenutzerklasse, während in einem anderen Unternehmen „Benutzer“ verwendet wird. Eine Richtlinie kann implementiert werden, um die Änderung an der Telefonnummer für eine `inetOrgPerson` im ersten Unternehmen hinzuzufügen. Ein andere Regel kann implementiert werden, durch die die Richtlinie für die Benutzerklasse angewendet werden kann. Richtlinien nehmen Schematranformationen vor, geben Übereinstimmungskriterien an, die festlegen, ob ein Objekt bereits im verbundenen System oder Identitätsdepot vorhanden ist, und führen viele andere Aufgaben aus. Daher könnte ein Ereignis vom Typ „Hinzufügen“, das vom verbundenen System gemeldet wurde, als ein Änderungsvorgang im Identitätsdepot enden, falls eine Übereinstimmungsrichtlinie festlegt, dass das von Ihnen hinzugefügte Objekt bereits im Identitätsdepot vorhanden ist.

Wenn im Abonnentenkanal ein neuer Benutzer im Identitätsdepot erstellt wird und Sie möchten, dass dies im verbundenen System geschieht, ruft die Identity Manager-Engine eine Reihe von Richtlinien auf, bevor dieser Befehl an den Treiber gesendet wird. Diese Richtlinien definieren die Art und Weise, wie Objekte erstellt werden, und legen fest, ob ein entsprechender Benutzer bereits im verbundenen System vorhanden ist. Sie treffen Entscheidungen zur Platzierung, liefern die Standardwerte für die erforderlichen Attribute, die nicht angegeben wurden, und so weiter. Dieses Ereignis vom Typ „Hinzufügen“ wird möglicherweise in ein Ereignis vom Typ „Ändern“ transformiert, wenn das Objekt im verbundenen System vorhanden ist. Attribute, die im ursprünglichen Ereignis nicht vorhanden waren, könnten hinzugefügt werden, um dem Objekterstellungsmodell des verbundenen Systems zu entsprechen.

Formatvorlagen definieren XSLT-Transformationsregeln. Formatvorlagen transformieren Eingabe- und Ausgabebefehle in verschiedene Befehle, ändern ein Ereignis von einem Typ in einen anderen, oder führen andere beliebige XML-Transformationen durch. Weitere Informationen hierzu finden Sie im Abschnitt Identity Manager-Formatvorlagen.

- Abschnitt 6.13.1, „Eingabetransformationsregel“, auf Seite 63
- Abschnitt 6.13.2, „Ausgabetransformationsregel“, auf Seite 63
- Abschnitt 6.13.3, „Verknüpfungen“, auf Seite 64

- Abschnitt 6.13.4, „Künstliches Hinzufügen“, auf Seite 64
- Abschnitt 6.13.5, „Verarbeitung der Zusammenführung“, auf Seite 66

6.13.1 Eingabetransformationsregel

Die Eingabetransformationsregel betrifft sowohl den Abonnentenkanal als auch den Herausgeberkanal. Der Zweck der Eingabetransformationsregel besteht darin, eine vorläufigeTransformation an allen XML-Dokumenten vorzunehmen, die vom verbundenen System an Identity Manager gesendet wurden und vom verbundenen System aus an Identity Manager zurückgesendet wurden. Die Eingabetransformationsregel wird auf die XML-Dokumente angewendet, die an `XmlCommandProcessor.execute` und `XmlQueryProcessor.query` gesendet werden, wenn sie vom verbundenen System aufgerufen werden. Sie wird auch auf die XML-Dokumente angewendet, die von `SubscriptionShim.execute` und `XmlQueryProcessor.query` zurückgesendet werden, wenn sie von der Identity Manager-Engine aufgerufen werden. Die Eingabetransformationsrichtlinie wird vor der Schemazuordnungsrichtlinie angewendet.

Die Eingabetransformationsregel wird oft verwendet, um Daten vom Anwendungsformat in das Identitätsdepotformat zu transformieren. Während die Eingabetransformation für Datenformattransformationen verwendet wird, führt die Ausgabetransformationsregel die Datentransformation normalerweise in die entgegengesetzte Richtung durch (das heißt, sie transformiert die Daten vom Identitätsdepotformat in das Anwendungsformat). Diese Regel wird in der Namespace der Anwendung aktiv. Sie könnte beispielsweise zum Neuformatieren von Daten verwendet werden, beispielsweise um eine Telefonnummer im Format 1(815)555-1212 in das Format 1-815-555-1212 zu ändern. Die Eingabetransformationsregel wird auch dazu verwendet, Aktionen durchzuführen als Antwort auf die Ergebnisse von Befehlen, die an das Schnittstellenmodul gesendet wurden. Schemanamen befinden sich immer in der Anwendungs-Namespace im XML-Dokument, das von der Eingabetransformationsrichtlinie verarbeitet wird. Es ist auch möglich, die Eingabetransformationsregel zu verwenden, um ein beliebiges natives XML-Format der verbundenen Anwendung in das von Identity Manager erwartete Format zu transformieren. Derartige Transformationen müssen in XSLT geschrieben werden, weil das DirXML-Skript nur mit dem XML-Vokabular arbeitet, das für Identity Manager spezifisch ist.

6.13.2 Ausgabetransformationsregel

Die Ausgabetransformationsrichtlinie betrifft sowohl den Abonnentenkanal als auch den Herausgeberkanal. Der Zweck der Ausgabetransformationsrichtlinie besteht darin, eine abschließende Transformation an allen XML-Dokumenten vorzunehmen, die von der Identity Manager-Engine an das Schnittstellenmodul gesendet und von Identity Manager an das Schnittstellenmodul zurückgesendet werden. Die Ausgabetransformationsrichtlinie wird auf die XML-Dokumente angewendet, die an `SubscriptionShim.execute` und `XmlQueryProcessor.query` gesendet werden, wenn sie von der Identity Manager-Engine aufgerufen werden. Sie wird auch auf die XML-Dokumente angewendet, die von `XmlCommandProcessor.execute` und `XmlQueryProcessor.query` zurückgesendet werden, wenn sie vom Schnittstellenmodul aufgerufen werden. Die Ausgabetransformationsregel wird nach der Schemazuordnungsrichtlinie angewendet.

Die Ausgabetransformationsregel ist die Umkehrung der Eingabetransformationsregel. Sie ändert den Befehl, der wie erforderlich an das Schnittstellenmodul übertragen werden soll. Dazu muss normalerweise das rückgängig gemacht werden, was in der Eingabetransformationsregel ausgeführt wurde. Wenn Sie beispielsweise eine Eingabetransformationsregel haben, die Telefonnummern im Format 1(815)555-1212 in das Format 1-815-555-1212 konvertiert, dann brauchen Sie eine Ausgabetransformationsregel, die 1-815-555-1212 ín 1(815)555-1212 konvertiert.

Sie können die Ausgabetransformationsrichtlinie auch für die Transformation von dem Format, das Identity Manager verwendet, in ein beliebiges natives XML-Format der verbundenen Anwendung verwenden. Diese Transformationen müssen in XSLT geschrieben werden, weil das DirXML-Skript nur mit dem XML-Vokabular arbeitet, das für Identity Manager spezifisch ist.

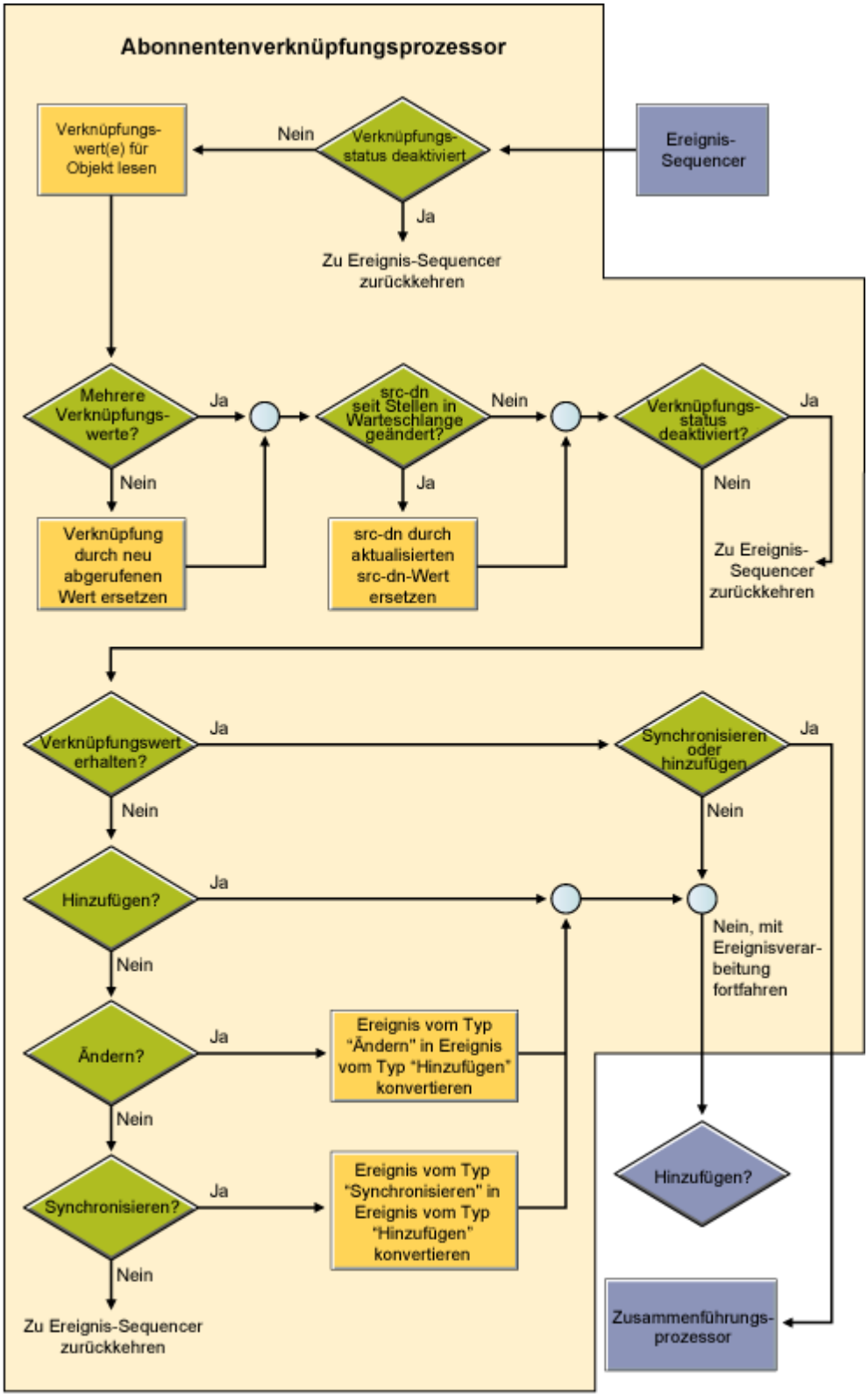
6.13.3 Verknüpfungen

Mit dem Wert „Verknüpfung“ bleibt Identity Manager auf dem Laufenden darüber, welches Objekt im verbundenen System mit einem Objekt im Identitätsdepot übereinstimmt. In fast allen Fällen sollte dies eine 1:1-Übereinstimmung sein, sodass man sagen kann, dass „john doe“, Mitarbeiter Nummer 1234567 im HR-System genau mit dem Benutzerobjekt „jdoe13“ im Identitätsdepot, mit „doe john“ in Active Directory und mit „jdoe13@example.com“ im Email-System übereinstimmt. Die meisten Computersysteme weisen einen internen eindeutigen Bezeichner auf. eDirectory und Active Directory verfügen über einen globalen eindeutigen Bezeichner (Globally Unique Identifier, GUID). Viele HR-Systeme verwenden eine Mitarbeiternummer. Email-Systeme weisen normalerweise einen eindeutigen Wert für die Email-Adresse jeder einzelnen Person auf. Identity Manager verwendet diese Bezeichner, um eine Verknüpfung zu erstellen. Verknüpfungen werden im Identitätsdepot gespeichert. Im Abonnentenkanal verwendet die Identity Manager-Engine diesen Wert, um es dem Schnittstellenmodul zu ermöglichen, das korrekte Objekt im verbundenen System zu ändern. Im Herausgeberkanal stellt das Schnittstellenmodul den Verknüpfungswert bereit und ermöglicht es der Identity Manager-Engine somit, das korrekte Objekt schnell und leicht im Identitätsdepot aufzufinden.

6.13.4 Künstliches Hinzufügen

Wenn der Änderungsvorgang keine Verknüpfung enthält, die bei Ankunft im Hinzufügeprozessor in ein tatsächliches Objekt aufgelöst wird, konvertiert die Identity Manager-Engine das Ereignis vom Typ „Ändern“ in einen Vorgang des künstlichen Hinzufügens. Die ist der Vorgang des künstlichen Hinzufügens und er kann sowohl im Herausgeber- als auch im Abonnentenkanal vorkommen. Die Identity Manager-Engine verwendet das Ereignis vom Typ „Ändern“, um herauszufinden, mit welchem Objekt sie arbeiten soll. Sie verwendet dann den Filter für Rückfragen, um alle Attribute abzurufen, die für dieses Objekt verfügbar und im aktuellen Kanal auf „Synchronisieren“ oder „Benachrichtigen“ festgelegt sind. Sie entfernt anschließend das Ereignis vom Typ „Ändern“ und erstellt ein Ereignis vom Typ „Hinzufügen“, das es ersetzt. Dieses Ereignis vom Typ „Hinzufügen“ wird dann durch die Übereinstimmungs-, Erstellungs-, Platzierungs- und Befehlstransformation geleitet (im Abonnenten durchläuft es außerdem noch die Schemazuordnung und Ausgabetransformation). Die Ereignistransformationsregel wird nicht für Vorgänge des künstlichen Hinzufügens ausgelöst. Der Grund dafür ist der Standort der Regel vor dem Hinzufügeprozessor.

Abbildung 6-4 *Verknüpfungsprozessor im Abonnentenkanal*



6.13.5 Verarbeitung der Zusammenführung

Ein Vorgang der Zusammenführung wird ausgeführt, wenn die Identity Manager-Engine einen Hinzufügevorgang in einen Änderungsvorgang konvertiert. Am häufigsten geschieht dies bei einer ursprünglichen Migration, weil durch die Migration Objekte entlang einem Kanal gesendet werden und die Übereinstimmungsregel ein Objekt findet, das es zur Verknüpfung mit dem zu migrierenden Objekt verwenden kann.

In einem Vorgang der Zusammenführung wird das aktuelle Dokument verworfen (wie das künstliche Hinzufügen), und der Filter wird verwendet, um sowohl das verbundene System als auch das Identitätsdepot nach allen Werten abzufragen. Die Einstellung für jedes Attribut im Filter wird verwendet, um zu entscheiden, was mit den Daten geschehen soll. Optional können die Quellinformationen mit den Informationen vom Ziel überschrieben, das Ziel mit der Quelle überschrieben, beide Methoden kombiniert und beide mit den Ergebnissen aktualisiert werden oder

es kann einfach nichts getan werden. Im folgenden Flussdiagramm sind der Zusammenführungsprozessor des Herausgebers und der Zusammenführungsprozessor des Abonnenten dargestellt.

Abbildung 6-5 *Zusammenführungsprozessor des Herausgebers*

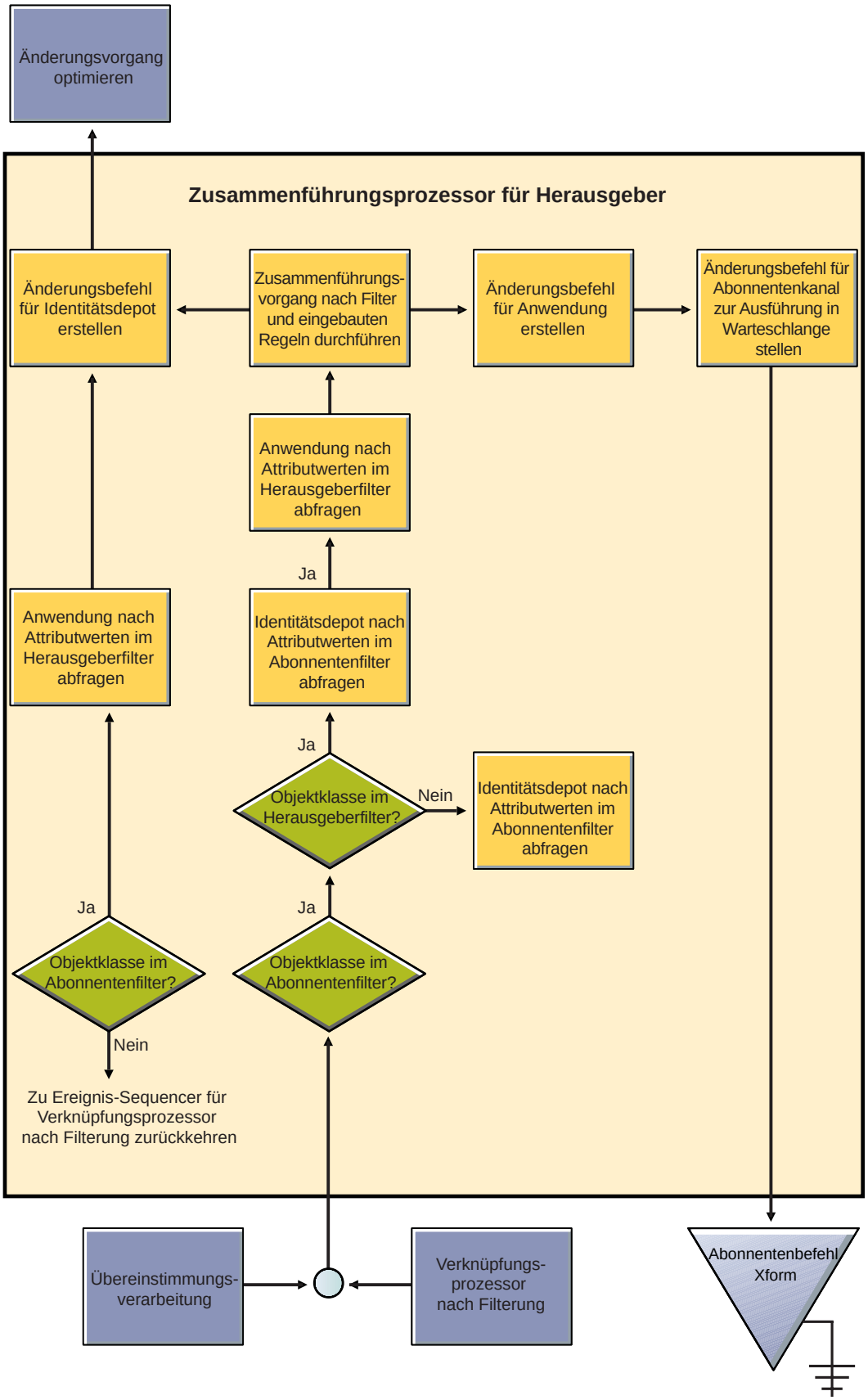
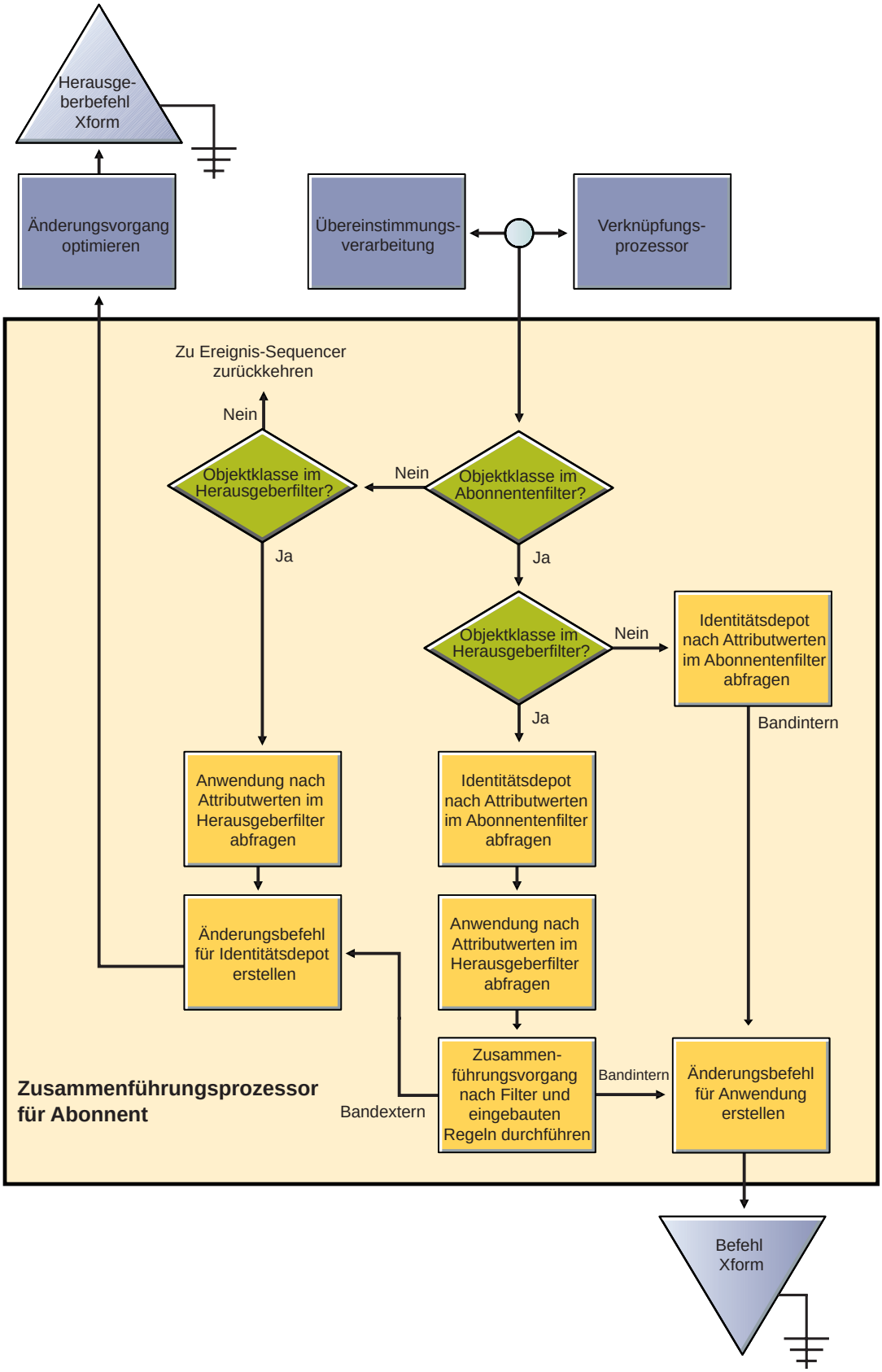

Änderungsvorgang optimieren
Zusammenführungsprozessor für Herausgeber
Änderungsbefehl für Identitätsdepot erstellen
Zusammenführungs-vorgang nach Filter und eingebauten Regeln durchführen
Änderungsbefehl für Anwendung erstellen
Änderungsbefehl für Abonnentenkanal zur Ausführung in Warteschlange stellen
Anwendung nach Attributwerten im Herausgeberfilter abfragen
Ja
Anwendung nach Attributwerten im Herausgeberfilter abfragen
Identitätsdepot nach Attributwerten im Abonnentenfilter abfragen
Ja
Objektklasse im Herausgeberfilter?
Nein
Identitätsdepot nach Attributwerten im Abonnentenfilter abfragen
Ja
Objektklasse im Abonnentenfilter?
Ja
Objektklasse im Abonnentenfilter?
Nein
Zu Ereignis-Sequencer für Verknüpfungsprozessor nach Filterung zurückkehren
Übereinstimmungs-verarbeitung
Verknüpfungs-prozessor nach Filterung
Abonnentenbefehl Xform

Abbildung 6-6 *Zusammenführungsprozessor des Abonnenten*



7 Weitere Schritte

Wenn Sie die Komponenten verstanden haben, aus denen Identity Manager 4.0.2 besteht, verwenden Sie im nächsten Schritt die Dokumentation, um Ihre eigene Identity Manager-Lösung zu erstellen. In den folgenden Abschnitten wird erläutert, wo die Dokumentation für die aufgeführten Aufgaben zu finden ist:

- Abschnitt 7.1, „Planen einer Identity Manager-Lösung“, auf Seite 71
- Abschnitt 7.2, „Vorbereiten der Daten für die Synchronisierung“, auf Seite 71
- Abschnitt 7.3, „Installation oder Aufrüstung von Identity Manager“, auf Seite 71
- Abschnitt 7.4, „Konfigurieren von Identity Manager“, auf Seite 72
- Abschnitt 7.5, „Identity Manager verwalten“, auf Seite 74

7.1 Planen einer Identity Manager-Lösung

Der erste Schritt beim Entwerfen einer Identity Manager-Lösung besteht darin zu entscheiden, was genau die Aufgabe der Lösung in Ihrem Unternehmen sein soll. Lesen Sie den Abschnitt „Planning“ (Planung) im *Identity Manager 4.0.2 Framework Installation Guide* (Installationshandbuch zu Identity Manager 4.0.1 Framework), um einen Plan für Ihre Identity Manager-Lösung mithilfe von Designer zu entwerfen. Sie können auch eine Benutzeranwendungs-Lösung erstellen. Verwenden Sie hierzu das *Benutzeranwendung: Designhandbuch*.

Mit Designer können Sie Informationen in einem Projekt erfassen und die Informationen für andere Personen freigeben. Sie können die Lösung im Designer zunächst modellieren, bevor Sie Änderungen vornehmen. Weitere Informationen über Designer finden Sie unter *Designer für Identity Manager*.

7.2 Vorbereiten der Daten für die Synchronisierung

Wenn Sie Ihren Plan erstellt haben, müssen Sie die Daten in Ihrer Umgebung für die Synchronisierung vorbereiten. Mithilfe von Analyzer analysieren und bereinigen Sie die Daten und bereiten diese für die Synchronisierung vor. Weitere Informationen hierzu finden Sie im *Analyzer 4.0.2 for Identity Manager Administration Guide* (Administrationshandbuch zu Analyzer 4.0.1 für Identity Manager).

7.3 Installation oder Aufrüstung von Identity Manager

Wenn Sie Ihren Plan erstellt und die Daten vorbereitet haben, können Sie Identity Manager installieren. Wenn Sie eine kleine bis mittlere IT-Umgebung haben und Identity Manager zum ersten Mal verwenden, ist es am besten, das integrierte Installationsprogramm zu verwenden. Das

integrierte Installationsprogramm installiert und konfiguriert alle in Identity Manager enthaltenen Komponenten. Weitere Informationen finden Sie im *Identity Manager 4.0.2 Integrated Installation Guide* (Handbuch zur integrierten Installation von Identity Manager 4.0).

Wenn Sie bereits über ein Identity Manager-System verfügen oder eine große IT-Umgebung haben, ziehen Sie das *Identity Manager 4.0.2 Framework Installationshandbuch* zu Rate, um die verschiedenen Identity Manager-Komponenten zu installieren bzw. aufzurüsten. Jede Identity Manager-Komponente wird separat installiert und konfiguriert, sodass Sie Ihre Identity Manager-Lösung an Ihre Anforderungen anpassen können.

- Installationsanweisungen finden Sie unter „Installation“ im *Identity Manager 4.0.2 Framework Installationshandbuch*.
- Aufrüstungsanweisungen finden Sie unter „Performing an Upgrade“ (Durchführen einer Aufrüstung) im *Identity Manager 4.0.2 Upgrade and Migration Guide* (Aufrüstungs- und Migrationshandbuch zu Identity Manager 4.0.1).
- Wenn Sie ein vorhandenes System auf neue Hardware migrieren, lesen Sie „Performing an Upgrade“ (Durchführen einer Aufrüstung) im *Identity Manager 4.0.2 Upgrade and Migration Guide* (Aufrüstungs- und Migrationshandbuch zu Identity Manager 4.0.1).
- Wenn Sie das rollenbasierte Bereitstellungsmodul (RBPM) migrieren müssen, lesen Sie nach im *Identity Manager 4.0.2: RBPM and Reporting Migration Guide* (Identity Manager 4.0.2: Handbuch zur RBPM- und Berichterstellungsmigration).

7.4 Konfigurieren von Identity Manager

Nach der Installation von Identity Manager müssen Sie verschiedene Komponenten konfigurieren, damit Sie eine voll funktionsfähige Lösung erhalten.

- Abschnitt 7.4.1, „Datensynchronisierung“, auf Seite 72
- Abschnitt 7.4.2, „Zuordnen von Rollen“, auf Seite 73
- Abschnitt 7.4.3, „Konfiguration der Benutzeranwendung“, auf Seite 73
- Abschnitt 7.4.4, „Konfigurieren von Revision, Berichterstellung und Konformität“, auf Seite 73

7.4.1 Datensynchronisierung

Identity Manager verwendet Treiber zum Synchronisieren von Daten zwischen verschiedenen Anwendungen, Datenbanken, Betriebssystemen und Verzeichnissen. Nach der Installation von Identity Manager müssen Sie einen oder mehrere Treiber für jedes System konfigurieren, mit dem Sie Daten synchronisieren möchten.

Zu jedem Treiber gibt es ein Handbuch, in dem die Anforderungen und Konfigurationsschritte erläutert werden, die zum Synchronisieren der Daten erforderlich sind. Die Treiberhandbücher befinden sich auf der Dokumentations-Website für Identity Manager 4.0.2 Treiber (http://www.netiq.com/documentation/idm402drivers/index.html).

Verwenden Sie das entsprechende Treiberhandbuch für jedes verwaltete System, um den Treiber zum Synchronisieren der Identitätsdaten zu erstellen.

7.4.2 Zuordnen von Rollen

Wenn Sie Informationen haben, die zwischen den verschiedenen Systemen synchronisiert werden müssen, verwenden Sie den Rollenzuordnungsadministrator zum Verwalten der Rollen in den verschiedenen Systemen. Weitere Informationen finden Sie im *Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide* (Benutzerhandbuch zum Novell Identity Manager-Rollenzuordnungsadministrator 4.0.2).

7.4.3 Konfiguration der Benutzeranwendung

Im nächsten Schritt fügen Sie mit der Benutzeranwendung eine Geschäftsperspektive zur Identity Manager-Lösung hinzu. Mit der Benutzeranwendung können Sie folgende Geschäftsanforderungen erfüllen:

- Anbieten einer praktischen Möglichkeit, rollenbasierte Bereitstellungsaktionen durchzuführen.
- Sicherstellen, dass Ihr Unternehmen über eine Methode verfügt, mit der es verifizieren kann, dass die Mitarbeiter die Unternehmensrichtlinien kennen und die erforderlichen Schritte unternehmen, um diese Richtlinien einzuhalten.
- Bereitstellen von Selbstbedienungsfunktionen, mit denen ein neuer Benutzer sich selbst registrieren kann, und Gewähren von Zugriff für anonyme oder Gastbenutzer.
- Sicherstellen, dass der Zugriff auf Unternehmensressourcen die organisatorischen Richtlinien erfüllt und dass die Bereitstellung im Kontext der Sicherheitsrichtlinie des Unternehmens erfolgt.
- Reduzierung des Verwaltungsaufwands für das Eingeben, Aktualisieren und Löschen von Benutzerinformationen über alle Systeme des Unternehmens hinweg.
- Verwalten der manuellen und automatisierten Bereitstellung von Identitäten, Diensten, Ressourcen und Assets.
- Unterstützung komplexer Workflows.

Das Handbuch *User Application: Administration Guide* (Benutzeranwendung: Administrationshandbuch) enthält Informationen zur Konfiguration dieser Funktionen der Benutzeranwendung.

7.4.4 Konfigurieren von Revision, Berichterstellung und Konformität

Der letzte und wichtigste Schritt beim Erstellen einer Identity Manager-Lösung besteht in der Konfiguration der Revisions-, Berichterstellungs- und Konformitätsfunktionen, um sicherstellen zu können, dass die Lösung Ihre Unternehmensrichtlinien einhält. Ziehen Sie folgende Handbücher für die Einrichtung und Konfiguration dieser Funktionen zu Rate:

- **Revision:** *Identity Manager 4.0.2 Berichterstellungshandbuch für Novell Sentinel*.
- **Berichterstellung:** *Handbuch zum Identitätsberichterstellungsmodul* und *Verwenden von Identity Manager 4.0.2 Berichten*.
- **Konformität:** Weitere Informationen finden Sie unter „Using the Compliance Tab“ (Verwenden der Registerkarte „Konformität“) im Handbuch *User Application: User Guide* (Benutzeranwendung: Administrationshandbuch).

7.5 Identity Manager verwalten

Wenn Ihre Identity Manager-Lösung vollständig ist, stehen viele Handbücher zur Verfügung, die Ihnen bei der Verwaltung, Pflege und Änderung Ihrer Identity Manager-Lösung entsprechend den sich ändernden und wachsenden Geschäftsanforderungen helfen. Die verschiedenen Administrationshandbücher sind auf der Identity Manager 4.0.2 Dokumentations-Website (http://www.netiq.com/documentation/idm402/index.html) im Bereich „Administration“ zu finden.